NETOPIA™ R3100 ISDN ROUTERS

User's Reference Guide
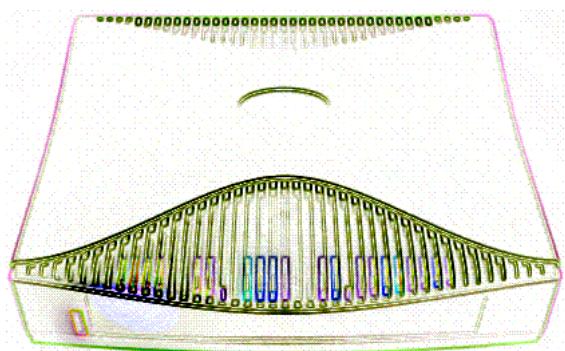
netopia®

Part Number

For additional copies of this electronic manual, order Netopia part number 6120343-PF-04

Printed copies

For printed copies of this manual, order Netopia part number TER3100/Doc
(P/N 6120343-00-04)

Contents

Welcome to the Netopia R3100 *User's Reference Guide*. This guide is designed to be your single source for information about your Netopia R3100 ISDN Router. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

This Table of Contents page you are viewing consists of hypertext links to the chapters and headings listed. If you are viewing this on-line, just click any link below to go to that heading.

Part II: Advanced Configuration

Configuration options for your Netopia R3100 ISDN Router

The Netopia R3100 ISDN Router can be used in different ways depending on your needs. In general, you will probably want to use it in one or more of the following ways: (Click on one of these links)

- "1. Small Office connection to the Internet" with several computers in your office sharing a single IP address (Network Address Translation enabled)

- "2. Small Office connection to the Internet" with a block of IP addresses (Network Address Translation disabled),

- "3. Direct Connection to a Corporate Office (Telecommuter)"

- "4. Configured to accept incoming dial-up connections"

- "5. Configured for IDSL"

This section is intended to give you a path to the appropriate installation and configuration instructions based on your intended use for the Netopia R3100 ISDN Router.

netopia®

1. Small Office connection to the Internet

For Small Office connections to the Internet, using a single dynamic IP address with Network Address Translation (NAT) enabled, you should use the following configuration option:

■ the SmartStart™ Wizard, included on your Netopia R3100 CD.
This is the fastest and simplest way to get you up and running with the minimum difficulty.

For instructions on this option, see "Setting up your Router with the SmartStart Wizard" on page 3-3.

netopia®

2. Small Office connection to the Internet

For Small Office connections to the Internet, using a block of IP addresses (Network Address Translation disabled), you use both of the following configuration tools:

■   the SmartStart™ Wizard, included on your Netopia R3100 CD.
    This is the fastest and simplest way to get you up and running with the minimum difficulty.

    For instructions on this option, see "Setting up your Router with the SmartStart Wizard" on page 3-3.

■   manual configuration using console-based management. This option allows maximum flexibility for experienced users and administrators.

    For instructions on this option, see "Console-based Management" on page 6-1.

netopia®

3. Direct Connection to a Corporate Office (Telecommuter)

For direct connections to a Corporate Office, you can use either one of two configuration options:

■ the SmartStart™ Wizard, included on your Netopia R3100 CD.

For instructions on this option, see "Setting up your Router with the SmartStart Wizard" on page 3-3.

■ manual configuration using console-based management. This option allows maximum flexibility for experienced users and administrators.

For instructions on this option, see "Console-based Management" on page 6-1.

netopia®

4. Configured to accept incoming dial-up connections

To configure the Netopia R3100 to accept incoming dial-up connections, you should use the following configuration option:

■ use the SmartStart™ Wizard, to configure your outbound connection to an ISP.

For instructions on this option, see "Setting up your Router with the SmartStart Wizard" on page 3-3.

■ manual configuration using console-based management. You will go to WAN configuration and add one or more dial-in Connection Profiles.

For instructions on this option, see "Creating a new Connection Profile" on page 8-1.

netopia®

5. Configured for IDSL

If you have the Netopia R3100-I IDSL model you can use either one of two configuration options:

■ the SmartStart™ Wizard, included on your Netopia R3100 CD.

For instructions on this option, see "Setting up your Router with the SmartStart Wizard" on page 3-3.

■ However, you may wish to skip directly to manual configuration using console-based management. This option allows maximum flexibility for experienced users and administrators, yet is very simple for the IDSL WAN interface.

For instructions on this option, see "IDSL Easy Setup" on page 7-6.

netopia®

Part I: Getting Started

Chapter 1

Introduction

Overview

The Netopia R3100 ISDN Router is a full-featured, stand-alone, multiprotocol router for connecting diverse local area networks (LANs) to the Internet and other remote networks. The Netopia R3100 ISDN Router uses a high performance telecommunications line to provide your whole network with a high-speed connection to the outside world.

This section covers the following topics:

■   "Features and capabilities" on page 1-1

■   "How to use this guide" on page 1-2

Features and capabilities

The Netopia R3100 ISDN Router provides the following features:

■   Support for IP and IPX routing for Internet and Intranet connectivity

■   IP address serving (over Ethernet or a WAN link) which allows local or remote network nodes to automatically acquire an IP address dynamically from a designated pool of available addresses

■   WAN connection over any ISDN phone line, including ISDN Digital Subscriber Lines (Ascend or Copper Mountain IDSL), switched, or leased,

■   ISDN wizard to automatically detect North American ISDN switch type, SPID, and with NI-1 support, directory numbers (DNs)

■   SmartPhone™ allows the router to use analog telephones or facsimile machines, saving the cost of adding separate telephone lines for these devices. More than Plain Old Telephone Service (POTS), SmartPhone adds distinctive ringing and CallerID capabilities.

■   Support for NI-1 ISDN advanced calling features (Hold, Drop, Transfer, and Conference) on POTS models

■   Auxiliary port support for remote console, LocalTalk, or WAN use (optional upgrades)

■   Dial-in RAS support over built-in ISDN channels or using optional add-on kit, on external analog modems (order TER/ADI)

■   Support for Ethernet LANs with multiple Ethernet IP subnets

■   Advanced ISDN cost control through scheduled connections and call accounting of both aggregate and

per-profile statistics

■ Console-based Telnet client

■ UNIX syslog client

■ Status lights (LEDs) for easy monitoring and troubleshooting

■ SmartStart™ Wizard software for easy configuration over an Ethernet network connection. The SmartStart Wizard may include an optional automatic registration with one of several major ISPs, making the process as simple as completing a registration form. Using the alternate manual setting to configure the router for an ISP that's not listed, the software allows you to configure your internal connection by entering just five fields: username, password, dialup number, DNS, and IP gateway.

■ Support for Console-based management

■ SmartIP™ for simple and economical to connect a workgroup of users to the Internet or a remote IP network by using Network Address Translation and a single IP address.

■ AppleTalk support (available as a separate add-on AppleTalk kit, including a firmware feature set enhancement and custom HD-15 dual RJ-11 PhoneNET™ connector) allows for LocalTalk to Ethernet routing in future firmware releases, assigning IP addresses to Macintosh users (MacIP), IP functionality for LocalTalk users, and AURP tunneling for connectivity between remote AppleTalk networks.

■ SmartView tool allows for real-time monitoring of router status lights (LEDs), through one or more information forms on a web-based Java applet. Internet browsers such as Netscape Navigator™ and Microsoft's Internet Explorer™ may be used for SmartView.

■ Wall-mountable, Bookshelf (Side-stackable), or Desktop-stackable design for efficient space usage

How to use this guide

In addition to the simple documentation contained in the accompanying documentation folio, this guide is designed to be your single source for information about your Netopia R3100 ISDN Router. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

You can also print out all of the manual, or individual sections, if you prefer to work from hard copy rather than on-line documentation. The pages are formatted to print on standard 8 1/2 by 11 inch paper. We recommend that you print on 3-hole punched paper, so that you can put the pages in a binder for future reference. For your convenience, a printed copy is available from Netopia. Order part number TER3100/Doc.

This guide is organized into chapters describing the Netopia R3100's advanced features. You may want to read each chapter's introductory section to familiarize yourself with the various features available.

Use the guide's table of contents and index to locate informational topics.

Chapter 2

Making the Physical Connections

This section tells you how to make the physical connections to your Netopia R3100 ISDN Router. This section covers the following topics:

- "Find a location" on page 2-1

- "What you need" on page 2-1

- "Identify the connectors and attach the cables" on page 2-2

- "Netopia R3100 ISDN Router Status Lights" on page 2-6

Find a location

When choosing a location for the Netopia Router, consider:

- Available space and ease of installation

- Physical layout of the building and how to best use the physical space available in relation to connecting your Netopia Router to the LAN

- Available wiring and jacks

- Distance from the point of installation to the next device (length of cable or wall wiring)

- Ease of access to the front of the unit for configuration and monitoring

- Ease of access to the back of the unit for checking and changing cables

- Cable length and network size limitations when expanding networks

For small networks, install the Netopia R3100 near one of the LANs. For large networks, you can install the Netopia R3100 in a wiring closet or a central network administration site.

What you need

Locate all items that you need for the installation.

Included in your router package are:

- The Netopia R3100 ISDN Router

- A power adapter and cord with a mini-DIN8 connector

- An Ethernet cable (RJ-45) to connect one computer to the built-in 10BaseT hub

- An ISDN cable (RJ-45) to attach to your Telco or Line port

- A dual DE-9 and mini-DIN8 to DE-9 console cable (to connect the router to either a PC or a Macintosh)

- The Netopia CD containing the SmartStart Wizard, this documentation, an Internet browser, Adobe®

Acrobat® Reader for Windows and Macintosh, ZTerm terminal emulator software and NCSA Telnet 2.6 for Macintosh

You will need:

■ A Windows 95, 98, or NT-based PC or a Macintosh with Ethernet connectivity for configuring the Netopia R3100. This may be built-in Ethernet or an add-on card, with TCP/IP installed.

■ An ISDN telephone line.

Identify the connectors and attach the cables

Identify the connectors and switches on the back panel and attach the necessary Netopia Router cables.
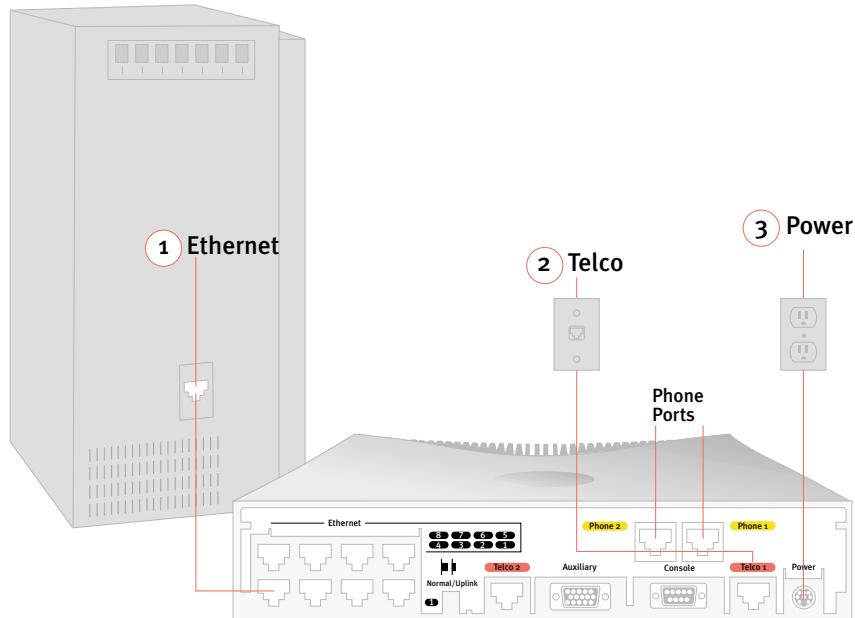
1. Connect one of the RJ-45 cables to any of the Ethernet ports on the router.

    (If you are connecting the router to an existing Ethernet hub, use Ethernet port #1 on the router and set the crossover switch to the **Uplink** position.)

2. Connect one end of one of the RJ-45 cables to the "Telco 1" or "Line 1" port, and the other end to your wall outlet.

3. Connect the mini-DIN8 connector from the Power Adapter to the Power port, and plug the other end into an electrical outlet.

    You should now have: the power adapter plugged in; the Ethernet cable connected between the router and your computer; and the telephone cables connected between the router and the wall outlets.

4. Insert your Netopia CD and follow the instructions to install an Internet browser and the Adobe Acrobat Reader, if you don't already have them.

Netopia R3100 ISDN Router Back Panel Ports

The figure below displays the back of the Netopia R3100 ISDN Router (models R3100-S, SP, U, UP).

Netopia R3100 ISDN Router back panel (models R3100 -S, SP, U, and UP)
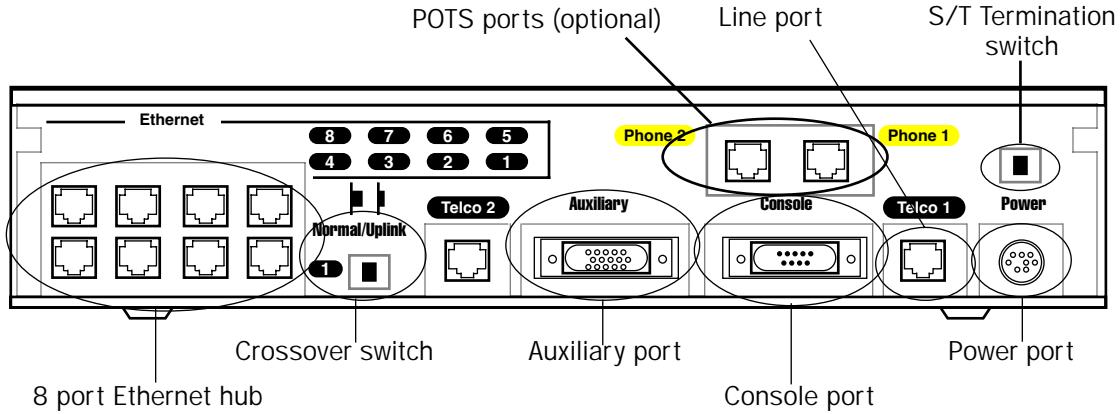
Note: For simplicity, the remainder of this manual uses the figure above to illustrate connections.

The figure below displays the back of the Netopia R3100 Router for Copper Mountain IDSL connections (R3100-I).

Netopia R3100 IDSL back panel (model R3100-I)
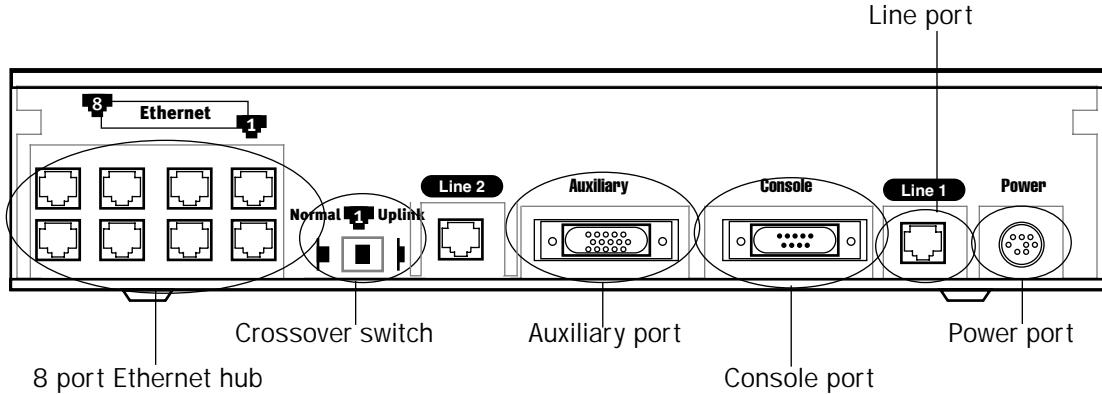
The following table describes all the Netopia R3100 ISDN Router back panel ports.

Port	Description
Power port	A mini-DIN8 power adapter cable connection.
Line or Telco port	A telephone-style jack labelled "Telco1" or "Line" for your WAN connection. Use the "Telco 1" or "Line 1" port, NOT "Telco 2" or "Line 2."
Console port	A DE-9 console port for a direct serial connection to the console screens. You can use this if you are an experienced user and don't want to use the preset 192.168.1.1 IP address in the router. See "Connecting a local terminal console cable to your router" on page 6-3.
Auxiliary port	An HD-15 auxiliary port for attaching an external modem or the optional AppleTalk kit.
Crossover switch	A crossover switch with Normal and Uplink positions. If you use Ethernet Port #1 for a direct Ethernet connection between a computer and the router, set the switch to the **Normal** position. If you are connecting the router to an Ethernet hub, use Ethernet port #1 on the router and set the switch to the **Uplink** position.
8-port Ethernet hub	Eight Ethernet jacks. You will use one of these to configure the Netopia R3100. For a new installation, use the Ethernet connection. You can either connect your computer directly to any of the Ethernet ports on the router, or connect both your computer and the router to an existing Ethernet hub on your LAN. Alternatively, you can use the console connection to run console-based management using a direct serial connection.
S/T Termination switch	Netopia R3100 S/T models also provide an S/T termination switch. The S/T termination switch on the Netopia R3100 back panel must be enabled to terminate the S/T bus. To enable this parameter, the switch must be toggled to the left.

Port	Description
2 Phone ports (POTS models only)	Netopia R3100 models that support SmartPhone™ provide two RJ-11 telephone jacks for connecting analog devices, such as a telephone, facsimile machine, or modem. * (UK users, see **Note** below) The POTS ports are configured by default to support call hold, call retrieve and the Flexible Call Offering (FCO) features known as Conference, Drop, and Transfer. ■ While a call is active, you can initiate a single flash hook (or if your phone is so equipped, press the Flash button) to start a second call. This will place the first call on hold, and provide a dial tone. Two individual active calls per channel are allowed. ■ Once the second call is established, you can switch back and forth between the two calls by sending a single flash hook. ■ If you want to conference two calls that are active (one on hold, and one live) send a double flash hook to activate the conference, followed by a single flash hook to bridge the calls together. This process can be repeated to bridge additional users to the conference, up to the maximum allowed by the line's provisioning. ■ If a conference is active, you can drop the last call added to the conference by issuing a double flash hook. ■ If you want to transfer an active conference (allow the two calls to continue to talk after the Netopia R3100 has disconnected), send a single flash hook to receive a new dial tone, followed by a double flash hook to initiate the transfer. For detailed configuration information, see "Using SmartPhone for Telephone Services" on page 9-1.

* Note: Users in the United Kingdom may need to obtain a special US-to-UK style modular connector adapter. Suitable adapters are available as follows:

Supplier	Phone No	Product Code
Black Box www.blackbox.co.uk	0118 9655100	MCU9413
Maplins Electronics www.maplin.co.uk	01702 554000	VD36

Netopia R3100 ISDN Router Status Lights

The figure below represents the Netopia R3100 status light (LED) panel.

Netopia R3100 LED front panel
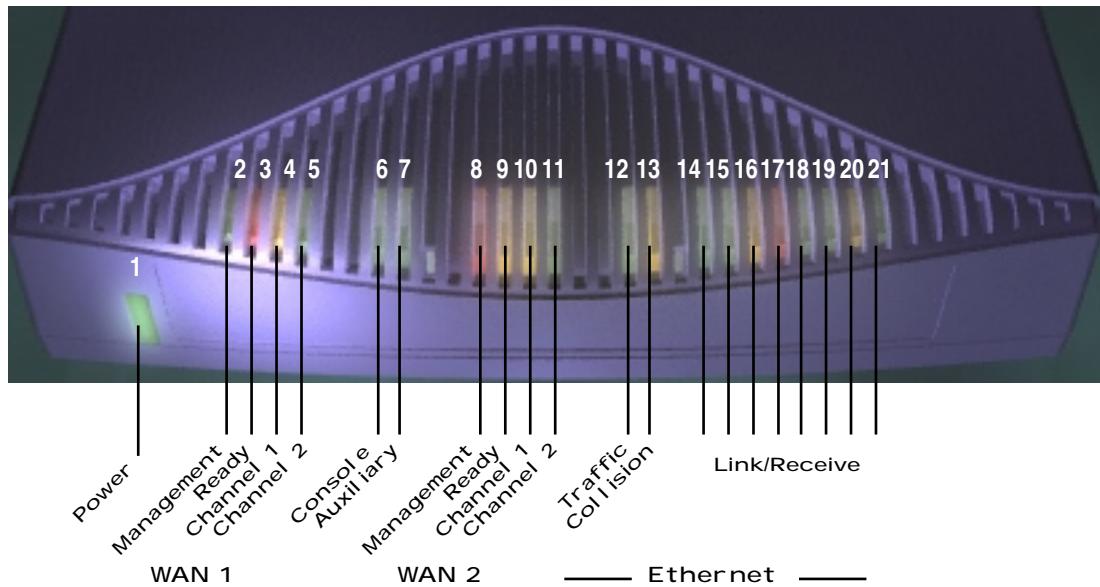
The following table summarizes the meaning of the various LED states and colors:

When this happens...	the LEDs...
Power is on	1 is **green**.
Data is transmitted or received over the ISDN D channel	2 flashes **orange**.
The WAN interface is operational	3 is **green**.
The WAN interface is inactive	3 is **off**.
The WAN interface detects a failure after line activation	3 flashes **red**.
Calls are setting up (voice or data)	4 and 5 flash **green**.
Data calls connect	4 and 5 are **green**.
Voice calls connect	4 and 5 flash **green**.
The line is carrying data traffic	4 and 5 pulse **orange**.
The respective Ethernet port is connected to the LAN	14 through 21 are **green**.
There is activity on the respective Ethernet ports	14 through 21 flash **green**.
Note: 8 through 11 are unused. Also, Console carrier (6) is ignored if the console is not configured for a remote modem.	

Chapter 3

Setting up your Router with the SmartStart Wizard

Once you've connected your router to your computer and your telecommunications line and installed a web browser, you're ready to run the Netopia SmartStart™ Wizard. The SmartStart Wizard will help you set up the router and share the connection. The SmartStart Wizard walks you through a series of questions and based on your responses automatically configures the router for connecting your LAN to the Internet or to your remote corporate network.

The SmartStart Wizard will:

■   automatically check your Windows 95, 98, or NT PC's TCP/IP configuration to be sure you can accept a dynamically assigned IP address, and change it for you if it is not set for dynamic addressing

■   check the physical connection from your computer to your router without your having to enter an IP address

■   assign an IP address to your router

■   allow you to register with a new ISP if you don't already have one (for analog modem and ISDN models). For a list of ISPs that support Netopia Routers in North America, see the Netopia website at http://www.netopia.com.

■   (for analog modem or ISDN models) allow you to enter your dial-up telephone numbers and other information, dial up and test your connection to your chosen ISP or other remote site

This chapter covers the following topics:

■   "Before running SmartStart" on page 2

■   "Setting up your Router with the SmartStart Wizard" on page 3

■   "Sharing the Connection" on page 10

Before running SmartStart

Be sure you have connected the cables and power source as described in Step 1 "Connect the Router" guide contained in your Netopia folio.

Before you launch the SmartStart application, make sure your computer meets the following requirements:

	PC	Macintosh
System software	Windows 95, 98, or NT operating system	MacOS 7.5 or later
Connectivity software	TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Windows 95, 98, or NT computers" on page 3-10	MacTCP or Open Transport TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Macintosh computers" on page 3-14.
Connectivity hardware	Ethernet card (10Base-T)	Either a built-in or third-party Ethernet card (10Base-T)
Browser software	Netscape Communicator™ or Microsoft Internet Explorer, included on the Netopia CD. Required for web-based registration and web-based monitoring.	
Notes: • The computer running SmartStart must be on the same Ethernet cable segment as the Netopia R3100. Repeaters, such as 10Base-T hubs between your computer and the Netopia R3100, are acceptable, but devices such as switches or other routers are not. • SmartStart for the PC will set your TCP/IP control panel to "Obtain an IP address automatically" if it is not already set this way. This will cause your computer to reboot. If you have a specified IP address configured in the computer, you should make a note of it before running SmartStart, in case you do not want to use the dynamic addressing features built in to the Netopia Router and need to restore the fixed IP address.		

Setting up your Router with the SmartStart Wizard

The SmartStart Wizard is tailored for your platform, but it works the same way on either a PC or a Macintosh. Insert the Netopia CD, and in the desktop navigation screen that appears, launch the **SmartStart Wizard** application.

SmartStart Wizard configuration screens

> The screens described in this section are the default screens shipped on the Netopia CD. They derive from two initialization (.ini) files included in the same directory as the SmartStart application file. Your reseller or your ISP may have supplied you with customized versions of these files.
>
> ■   If you have received a CD or diskette that has been customized by your reseller or ISP, you can run the SmartStart Wizard directly from the CD or diskette and follow the instructions your reseller or ISP provides. This makes your Netopia R3100 configuration even easier.
>
> ■   If you have received only the .ini files from your reseller or ISP, perform the following:
>
> > ■   Copy the entire directory folder containing the SmartStart Wizard application from the Netopia CD to your hard disk.
> >
> > ■   Copy the customized .ini files to the same directory folder that contains the SmartStart Wizard application, allowing the copy process to overwrite the original .ini files.
> >
> > ■   Run the SmartStart Wizard from your hard disk. You can then follow the instructions your reseller or ISP provides.

The SmartStart Wizard presents a series of screens to guide you through the preliminary configuration of a Netopia R3100. It will then create a connection profile using the information you supply to it.

Welcome screen. The first screen welcomes you to the SmartStart Wizard configuration utility.

Click the **Next** button after you have responded to the interactive prompts in each screen.

The **Help** button will display useful information to assist you in responding to the interactive prompts.

Easy or Advanced options screen. You can choose either **Easy** or **Advanced** setup.

■   If you choose **Easy**, SmartStart automatically uses the preconfigured IP addressing setup built into your router. This is the best choice if you are creating a new network or don't already have an IP addressing scheme on your new network.

   If you choose Easy, you will see a "Connection Test screen," like the one shown below while SmartStart checks the connection to your router.

■   If you choose **Advanced**, skip to page 3-9 now. The SmartStart Wizard displays the "Router IP Address screen" on page 3-9, in which you can choose ways to modify your router's IP address.
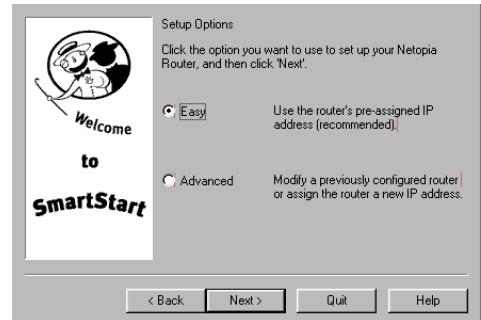
Easy option

Connection Test screen. SmartStart tests the connection to the router. While it is testing the connection, a progress indicator screen is displayed and the router's Ethernet LEDs flash.

When the test succeeds, SmartStart indicates success.

If the test fails, the wizard displays an error screen. If the test fails, check the following:

■   Check your cable connections. Be sure you have connected the router and the computer properly, using the correct cables. Refer to the Step 1 "Connect the Router" sheet in your Netopia R3100 documentation folio.

■   Make sure the router is turned on and that there is an Ethernet connection between your computer and the router.

■   Check the TCP/IP control panel settings to be sure that automatic IP Addressing (Windows) or DHCP (Macintosh) is selected. If you are using a Windows PC, SmartStart will automatically detect a static IP address and offer to configure the computer for automatic addressing. On a Macintosh computer, you must manually set the TCP/IP Control Panel to DHCP. See "Configuring TCP/IP on Macintosh computers" on page 3-14. If you currently use a static IP address outside the 192.168.1.x network, and want to continue using it, use the Advanced option to assign the router an IP address in your target IP range. See "Advanced option" on page 3-9.

■   If all of the above steps fail to resolve the problem, reset the router to its factory default settings and rerun

SmartStart. See the on-line *User's Reference Guide* for instructions.

When the test is successful, SmartStart presents you with a different screen, depending on the type of router you are configuring.

■   If you are configuring a router that defaults to an unswitched interface, such as **IDSL**, you will see the "Additional Configuration screen," shown below.

Additional Configuration screen. If you have a router that has a permanent unswitched connection to your ISP, such as an IDSL, SDSL, or Ethernet WAN interface router attached to a cable modem, the Additional Configuration screen appears.

You may want to do additional configuration to customize your network environment. SmartStart lets you launch your Telnet application. Click the Telnet button to launch your Telnet application.

Advanced configuration options available via Telnet are explained in "Console-based Management" on page 6-1.

However, if you need no further configuration options, click **Quit**. Congratulations! You're done!
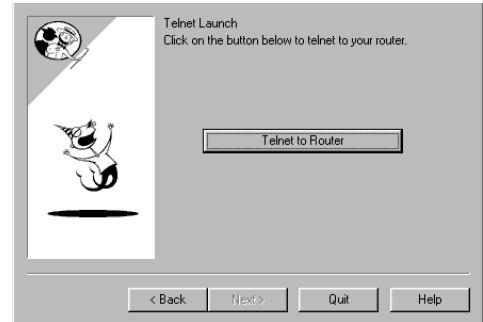
■   If you are configuring an **ISDN router**, you may see the "ISDN Switch Type screen," shown below, displaying the possible switch types available for your region. This screen may not appear, if there is only one switch type in use in your region or you are using a customized version of SmartStart, or the ISDN Wizard has automatically detected your switch type.

ISDN Switch Type screen. If you have an ISDN router, the ISDN Switch Type screen appears.

Select one of the supported ISDN switch types for your ISDN line. Your telephone company should have provided this information when your ISDN line was installed.

When you have done this, click **Next**.

Note: The switch types listed are different for different regions. If your region has only one switch type, this screen may not appear. In that case, skip to "Additional ISDN Configuration screen" on page 3-6.
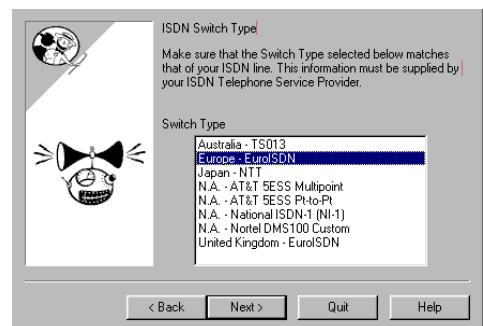
Additional ISDN Configuration screen. For ISDN dial-up connections, enter your Directory Numbers (DNs) and for North America only, Service Profile Identifiers (SPIDs).

Your telephone company should have provided this information on an information sheet when your ISDN line was installed.

If no additional ISDN configuration information is needed, this screen will not appear. Skip to "Manual or Automated Connection Profile screen" on page 3-6 below.

Note: For some switch types, or if you have an international router without the SmartPhone feature, fewer fields are shown in this screen.

When you have done this, click **Next**.

The "Manual or Automated Connection Profile screen" on page 3-6 shown below will appear.

■   If you are configuring an **ISDN** or a **Dual Analog router**, you will see the "Manual or Automated Connection Profile screen," shown below.

Manual or Automated Connection Profile screen. The SmartStart Wizard asks you to select a method of creating a connection profile. The connection profile tells your router how to communicate with your ISP or other remote site, such as your corporate office. You can select either **ISP Automation** or **Manual Entry**.

Options are explained below.

Make your selection and click **Next**.
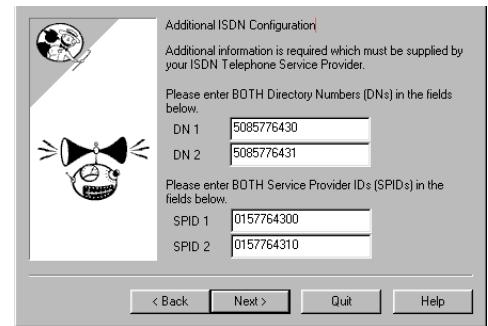
If you select **ISP Automation**, SmartStart offers you the option of choosing one of several Netopia ISP partners that support the Netopia R3100. You then see the "Internet Service Provider Selection screen" on page 3-7.

If you select **Manual Entry**, you must be prepared with the following information. You must enter:

■   Your dial-up number, sometimes referred to as an ISP POP number

■   Your Login name and Password. (These are case-sensitive.)

■   Any PBX or Centrex phone system dialing prefix (such as "9" for an outside line)

■   Your PPP authentication method. Options are: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or None. Most ISPs use PAP; this is the default.

■   Your Domain Name Server (DNS); this entry must be an IP address in dotted decimal format. (for example, 192.168.4.10, not "joe.isp.com")

■   Optionally, an alternate DNS if your ISP provided one

If you select Manual Entry, the "Connection Profile screen," shown below appears.

Internet Service Provider Selection screen. Select an
ISP from the list of Netopia ISP partners who have
provided information for automatic setup. Choose
Generic ISP if your ISP is not included on the list. If you
don't already have an account with the selected ISP, call
and order service using the listed customer service
telephone number.

When you have done this, click **Next**.
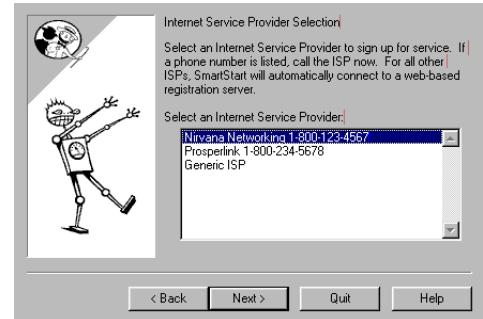
■   Most ISPs will provide you with information for you to enter in the "Connection Profile screen" on page 3-7
(shown below) over the phone using the toll-free phone number shown in the scrolling list. Generally, they
will provide you with:

■   Your dial-up number, sometimes referred to as an ISP POP number

■   Your Login name and Password. (These are case-sensitive.)

Note: Your ISP may provide you with additional values such as "Remote IP Gateway" or "Subnet Mask."
These entries are not required for the SmartStart Wizard to configure your router.

If you have a PBX or Centrex phone system, you may need a dialing prefix (such as "9" for an outside line).
You will enter that information in the "Connection Profile screen," shown below.

Connection Profile screen. Enter your ISP-supplied
configuration information mentioned above. All fields
must be filled in except the Alternate DNS field if your ISP
does not provide one. If your ISP appeared in the
"Internet Service Provider Selection screen" on page 3-7
your ISP will already have provided much of the
information required for the connection, and these fields
will appear grayed-out.

When you have done this, click **Next**.

The "Name and Password screen" on page 3-8 appears;
this is where you enter the username and password for
your connection to your ISP.
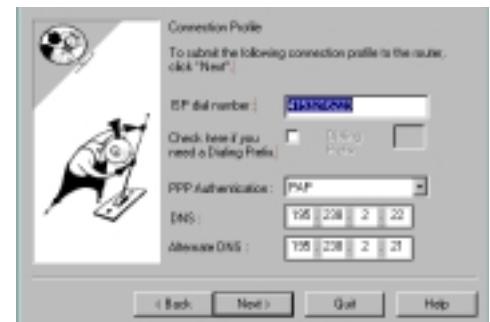
Name and Password screen. Enter the username and password that identifies you to your ISP.

Note: Some automated profiles already specify name and password for you. in this case, the screen is filled out for you and automatically skipped.

When you have done this, click **Next**.

The SmartStart Wizard then posts your connection profile information to your router.

Now the "Connection Profile Test screen," (shown below) appears. It allows you to test your connection to your ISP using the connection profile you have just created.

Connection Profile Test screen. SmartStart tests your connection profile by attempting to connect to your ISP.

To test the connection profile with your ISP, click **Next**.

While the test is running, SmartStart reports its progress in a brief succession of dialog boxes as described below.

Available Line Test Progress screen. SmartStart tests to see if the router can place calls on your telephone line. While it is testing the connection, a dialog box is displayed and the LEDs flash.

Connection Test Progress screen. SmartStart displays a dialog box showing you that your connection profile is being tested. If this test fails, check the physical connections between the computer, the router, and the wall jack or jacks. Check for errors in any manual entries you made during the configuration process.

Final screen. When the connection tests successfully, SmartStart displays a screen telling you that your configuration is now complete.

In most cases, this SmartStart configuration is all that you need to get your router up and running and connected to the Internet. However, you may want to take advantage of additional features or special configuration options available through the console-based configuration interface. For detailed instructions, see "Console-based Management" on page 6-1.

Advanced option

Router IP Address screen. If you selected the Advanced option in the "Easy or Advanced options screen" on page 3-4, SmartStart asks you to choose between entering the router's current IP address and assigning an IP address to the router.

If the router has already been assigned an IP address, select the first radio button. If you do this, the "Known IP Address screen," appears (shown below.)

If you want to reconfigure the router with a new IP address and subnet mask, select the second radio button. If you do this, the "New IP Address screen" on page 3-10 appears.

When you have done this, click **Next**.

Known IP Address screen. SmartStart displays a recommended address for the router based on the IP address of the computer.

If you know the router has an IP address different from the default value, enter it now. Otherwise, accept the recommended address.

When you have done this, click **Next**.

SmartStart tests the connection to your router.

SmartStart then returns you to an "Additional Configuration screen" on page 3-5.
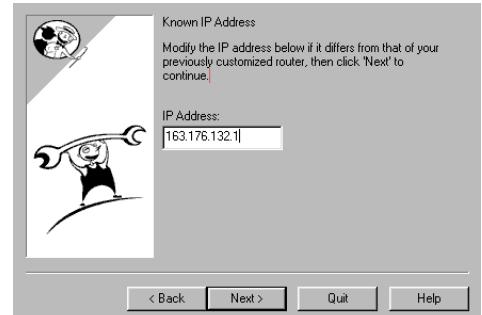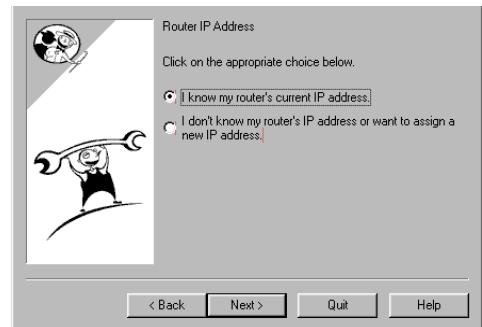
New IP Address screen. If you want to change the router's IP address, you enter the new IP address, the subnet mask, and the router's serial number in this screen. Remember, the serial number is on the bottom of the router. It is also found in your documentation folio.

Note: Forcing a new IP address may turn off the Netopia R3100's IP address serving capabilities, if you assign an IP address and subnet mask outside the router's current IP address serving pool. The Netopia R3100 does not allow an invalid address to be served. Use this option with caution.

When you have done this, click **Next**.

SmartStart forces the new IP address into the router, tests the connection, and then resets the router.

SmartStart then returns you to the "Manual or Automated Connection Profile screen" on page 3-6.
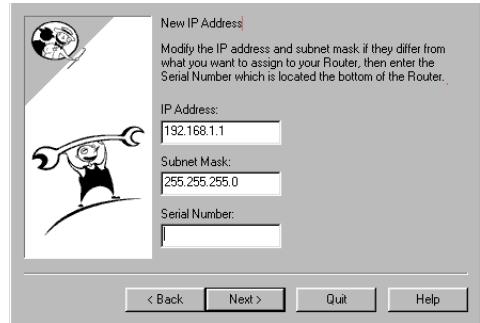
Sharing the Connection

Configuring TCP/IP on Windows 95, 98, or NT computers

Configuring TCP/IP on a Windows computer requires the following:

■   An Ethernet card (also known as a network adapter)

■   The TCP/IP protocol must be "bound" to the adapter or card

Dynamic configuration (recommended)

If you configure your Netopia R3100 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP) server, which enables dynamic addressing, is enabled by default in the router. If your PC is not set for dynamic addressing, SmartStart will offer to do this for you when you launch it. In that case, you will have to restart your PC and relaunch SmartStart. If you configure your PC for dynamic addressing in advance, SmartStart need only be launched once. To configure your PC for dynamic addressing do the following:
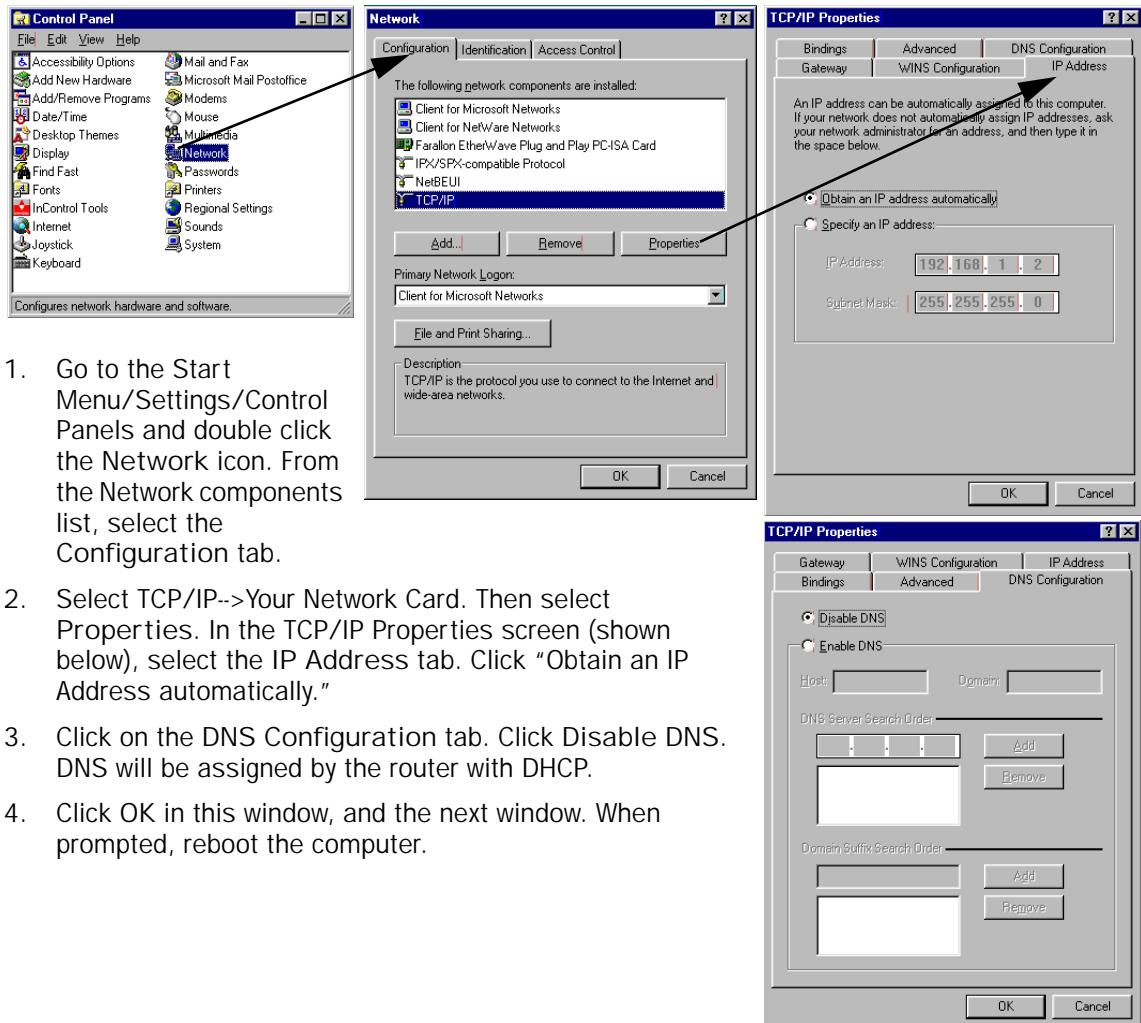
1. Go to the Start Menu/Settings/Control Panels and double click the **Network** icon. From the Network components list, select the **Configuration** tab.

2. Select TCP/IP-->Your Network Card. Then select **Properties**. In the TCP/IP Properties screen (shown below), select the **IP Address** tab. Click "Obtain an IP Address automatically."

3. Click on the **DNS Configuration** tab. Click **Disable DNS**. DNS will be assigned by the router with DHCP.

4. Click **OK** in this window, and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia R3100.

Static configuration (optional)

If you are manually configuring for a fixed or static IP address, perform the following:

1. Go to Start Menu/Settings/Control Panels and double click the **Network** icon. From the Network components list, select the **Configuration** tab.

2. Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the **IP Address** tab. Click "Specify an IP Address."
    Enter the following:
    IP Address: 192.168.1.2
    Subnet Mask: 255.255.255.0
    This address is an example of one that can be used to configure the router with the Easy option in the SmartStart Wizard. Your ISP or network administrator may ask you to use a different IP address and subnet mask.
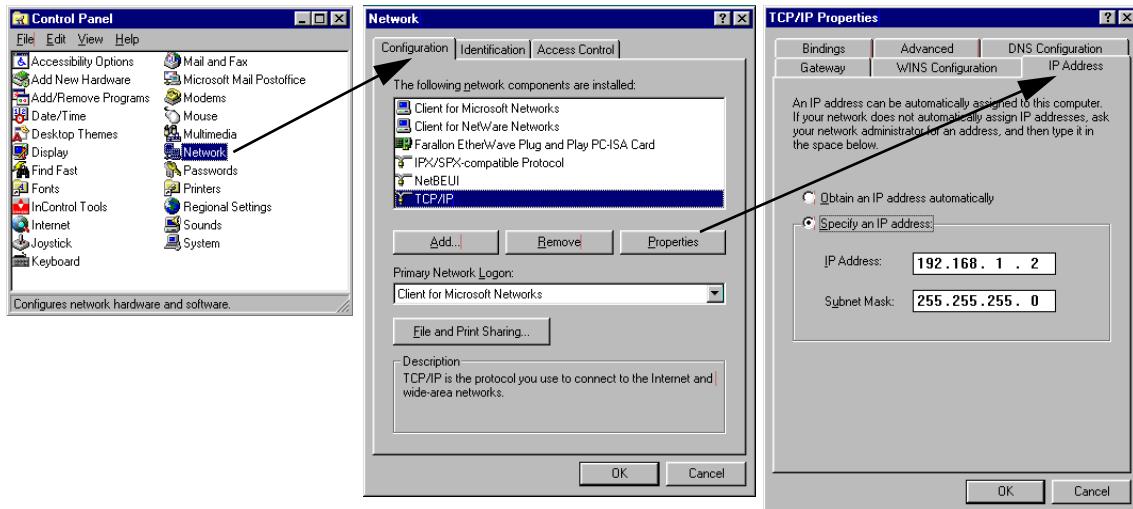
3. Click on the **Gateway** tab (shown below). Under "New gateway," enter **192.168.1.1**. Click **Add**. This is the Netopia R3100's pre-assigned IP address.
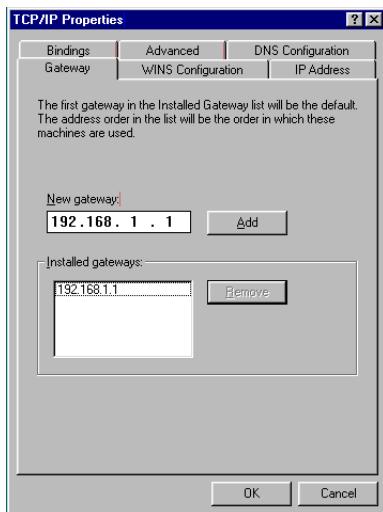
Click on the **DNS Configuration** tab. Click **Enable DNS**. Enter the following information:

Host: Type the name you want to give to this computer.

Domain: Type your domain name. If you don't have a domain name, type your ISP's domain name; for example, netopia.com.

DNS Server Search Order: Type the primary DNS IP address given to you by your ISP. Click **Add**. Repeat this process for the secondary DNS.

Domain Suffix Search Order: Enter the same domain name you entered above.
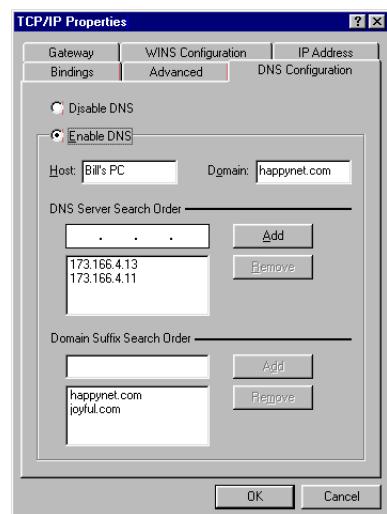
4. Click **OK** in this window, and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Configuring TCP/IP on Macintosh computers

The following is a quick guide to configuring TCP/IP for MacOS computers. Configuring TCP/IP in a Macintosh computer requires the following:

■ You must have either Open Transport or Classic Networking (MacTCP) installed.

   Note: If you want to use the Dynamic Host Configuration Protocol (DHCP) server built into your Netopia R3100 to assign IP addresses to your Macintoshes, you must be running Open Transport, standard in MacOS 8, and optional in earlier system versions. You can have your Netopia R3100 dynamically assign IP addresses using MacTCP; however, to do so requires that the optional AppleTalk kit be installed which can only be done after the router is configured.

■ You must have built-in Ethernet or a third-party Ethernet card and its associated drivers installed in your Macintosh.

Dynamic configuration (recommended)

If you configure your Netopia R3100 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP), which enables dynamic addressing, is enabled by default in the router. To configure your Macintosh computer for dynamic addressing do the following:

1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP**.

2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Basic** and click **OK**.

3. In the TCP/IP window, select "Connect via: Ethernet" and "Configure: Using DHCP Server."
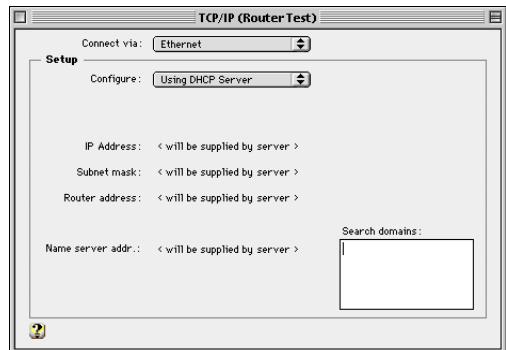
Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia R3100.

Static configuration (optional)

If you are manually configuring for a fixed or static IP address, perform the following:

1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP** or **MacTCP**.

2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**.

    Or, in the MacTCP window, select **Ethernet** and click the **More** button.
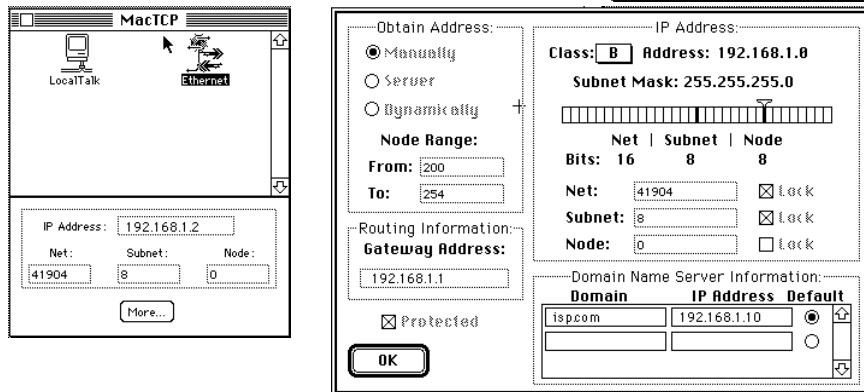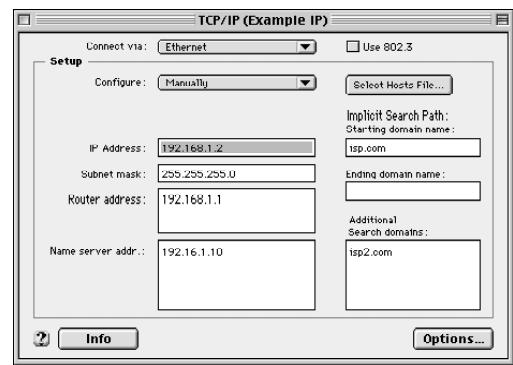
3. In the TCP/IP window or in the MacTCP/More window, select or type information into the fields as shown in the following table.

Option:	Select/Type:
Connect via:	Ethernet
Configure:	Manually
IP Address:	192.168.1.2
Subnet mask:	255.255.255.0
Router address:	192.168.1.1
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

4. Close the TCP/IP or MacTCP control panel and save the settings.

5. If you are using MacTCP, you must restart the computer. If you are using Open Transport, you do not need to restart. These are the only fields you need to modify in this screen.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Dynamic configuration using MacIP (optional)

If you want to use MacIP to dynamically assign IP addresses to the Macintosh computers on your network you must install the optional AppleTalk feature set kit.

Note: You cannot use MacIP dynamic configuration to configure your Netopia R3100 ISDN Router because you must first configure the router in order to enable AppleTalk.

Once the AppleTalk kit is installed, you can configure your Macintoshes for MacIP. To configure dynamically using MacIP, perform the following:

Using Open Transport TCP/IP

1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP**.

2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**.
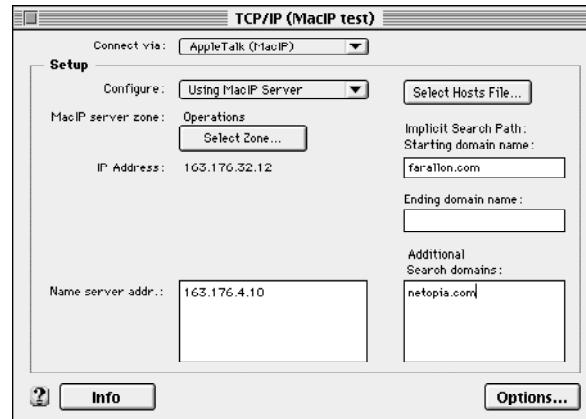
3. In the TCP/IP window, select or type information into the fields as shown in the following table.

TCP/IP Option:	Select/ Type:
Connect via:	AppleTalk (MacIP)
Configure:	Using MacIP server
MacIP Server zone:	(select available zone)
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

4. Close the TCP/IP control panel and save the settings.

    These are the only fields you need to modify in these screens.

Using Classic Networking (MacTCP)

1. Go to the Apple Menu. Select **Control Panels** and then **Network**.

2. In the Network window, select **EtherTalk**.
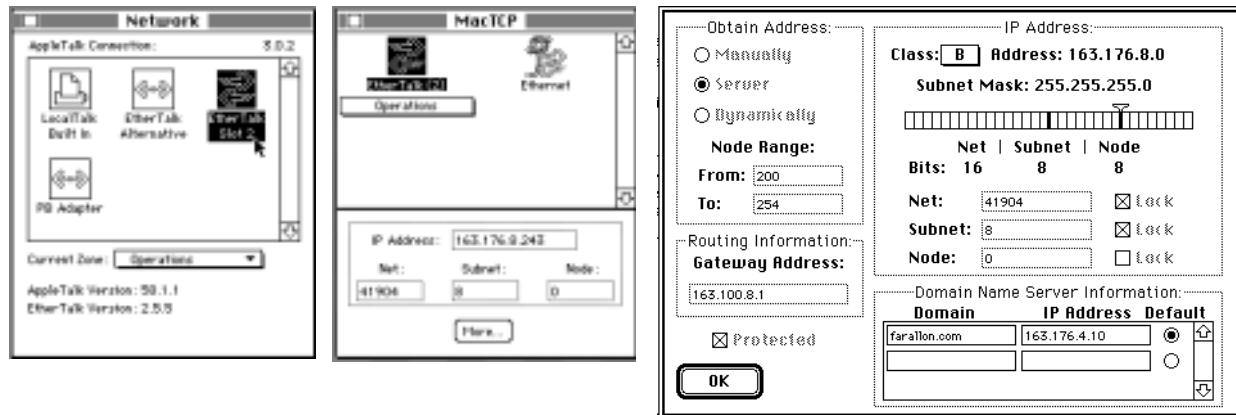
3. Go back to the Apple menu. Select **Control Panels** and then **MacTCP**.

4. Select **EtherTalk**.

   From the pull-down menu under EtherTalk, select an available zone; then click the **More** button.

   In the MacTCP/More window select the **Server** radio button. If necessary, fill in the Domain Name Server Information given to you by your administrator.

5. Restart the computer.

   These are the only fields you need to modify in these screens.

Note: More information about configuring your Macintosh computer for TCP/IP connectivity through a Netopia R3100 can be found in Technote NIR_026, "Open Transport and Netopia Routers," located on the Netopia Web site.

Chapter 4

Connecting Your Local Area Network

This chapter describes how physically to connect the Netopia R3100 ISDN Router to your local area network (LAN). Before you proceed, make sure the Netopia R3100 is properly configured. You can customize the Router's configuration for your particular LAN requirements using Console-based Management (see "Console-based Management" on page 6-1).

This section covers the following topics:

- "Overview" on page 4-1

- "Readying computers on your local network" on page 4-2

- "Connecting to an Ethernet network" on page 4-3

- "Remote console" on page 4-5

- "Connecting to a LocalTalk network" on page 4-6

Overview

You can connect the Netopia R3100 to an IP or IPX network that uses Ethernet.

If you have purchased the AppleTalk feature expansion kit (order Netopia P/N TER/ATI), you can also connect the Router to a LocalTalk network that uses PhoneNET cabling. On Netopia R3100 ISDN Routers, the AppleTalk kit LocalTalk features require minimum firmware version 4.3.

See the sections later in this chapter for details on how to connect the Netopia R3100 to different types of networks.

Readying computers on your local network

PC and Macintosh computers must have certain components installed before they can communicate through the Netopia R3100. The following illustration shows the minimal requirements for a typical PC or Macintosh computer.

```
┌─────────────────────────────────────────┐
│           Application software            │
├─────────────────────────────────────────┤
│              TCP/IP stack                 │
├─────────────────────────────────────────┤
│   Ethernet/EtherTalk/LocalTalk Driver     │
└─────────────────────────────────────────┘
```

Your PC
or Macintosh
computer

To the Netopia R3100
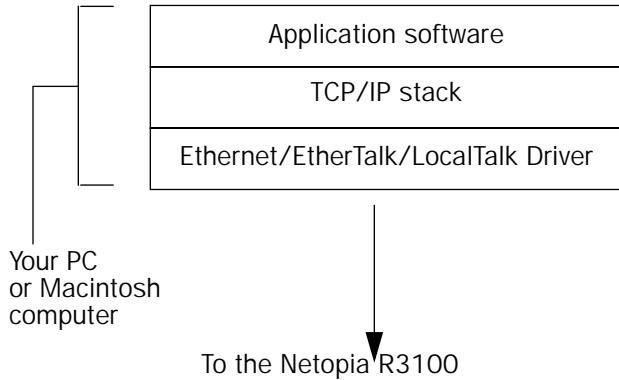
Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora e-mail client, and the web browsers Microsoft Internet Explorer and Netscape Navigator.

TCP/IP stack: This is the software that lets your PC or Macintosh communicate using Internet protocols. TCP/IP stacks must be configured with some of the same information you used to configure the Netopia R3100. There are a number of TCP/IP stacks available for PC computers. Windows 95 includes a built-in TCP/IP stack. See "Configuring TCP/IP on Windows 95, 98, or NT computers" on page 3-10. Macintosh computers use either MacTCP or Open Transport. See "Configuring TCP/IP on Macintosh computers" on page 3-14.

Ethernet: Ethernet hardware and software drivers enable your PC or Macintosh computer to communicate on the LAN.

EtherTalk and LocalTalk: These are AppleTalk protocols used over Ethernet. LocalTalk support is available as an optional feature set upgrade.

Once the Netopia R3100 is properly configured and connected to your LAN, PC and Macintosh computers that have their required components in place will be able to connect to the Internet or other remote IP networks.

Connecting to an Ethernet network

The Netopia R3100 supports Ethernet connections through its eight Ethernet ports. The Router automatically detects which Ethernet port is in use.

You can connect either 10Base-T or 10/100 Ethernet networks to the Netopia R3100.

10Base-T

You can connect a standard 10Base-T Ethernet network to the Netopia R3100 using any of its available Ethernet ports.

Netopia R3100 back panel

8 port Ethernet hub
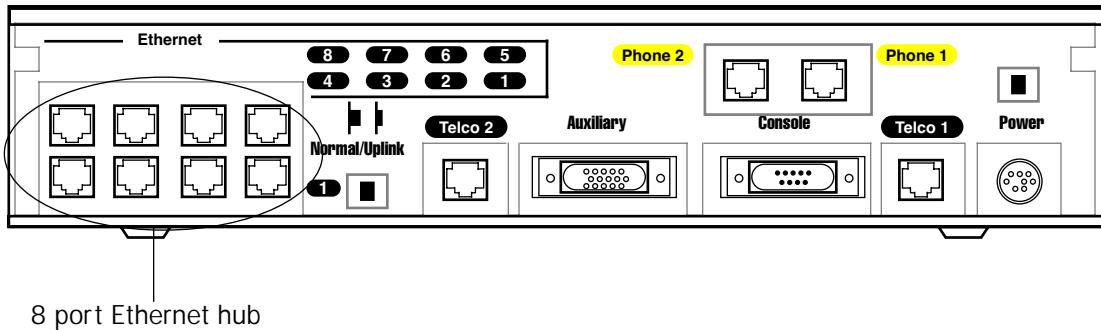
The Netopia R3100 in a 10Base-T network
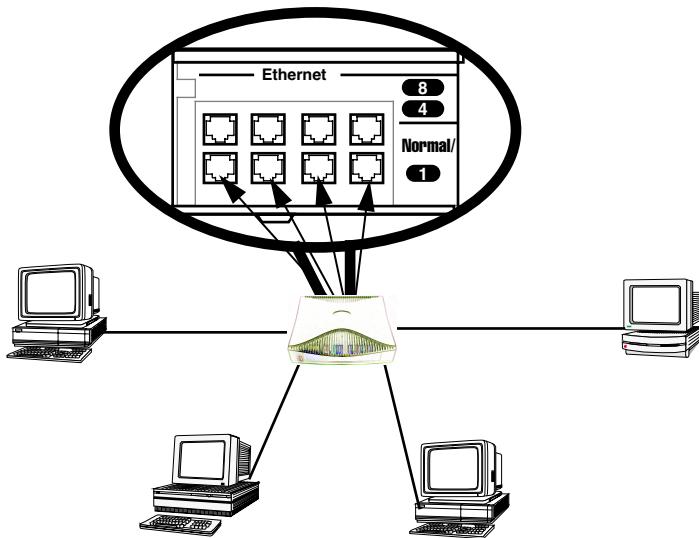
To connect your 10Base-T network to the Netopia R3100 through an Ethernet port, use a 10Base-T cable with RJ-45 connectors.

If you have more than eight devices to connect, you can attach additional devices using either a 10Base-T hub or an EtherWave daisy chain, or some combination of both.

■   If you add devices connected through a 10 Base-T or 10/100 Ethernet hub, connect the hub to Ethernet port number 1 on the Netopia R3100 and set the Normal/Uplink switch to Uplink.

When there are no more free ports on the 10Base-T hub, the network can be extended using EtherWave, a daisy-chainable Ethernet solution from Farallon.
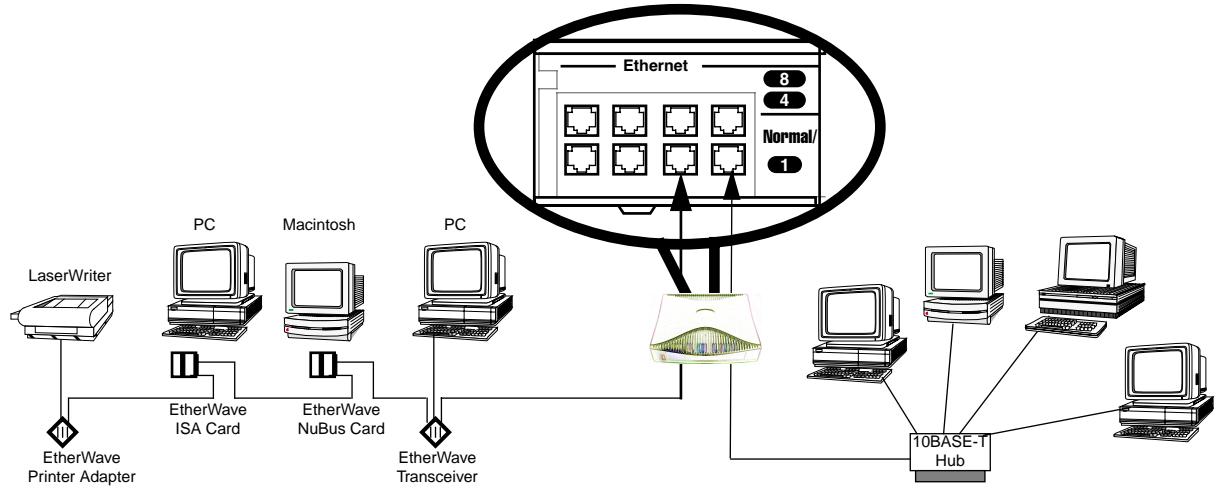
Remote console

You may want to add an external modem to your Auxiliary port. Remote modem terminal emulator setups can dial in to the modem line and establish a remote console session. This allows an administrator with the appropriate security to remotely configure your router for you.

Obtain the special external modem cable (Netopia Part Number TE6/DB25) either from your reseller or directly from Netopia. Refer to the sheet of optional feature set add-ons in your Netopia R3100 documentation folio.

Netopia R3100 Auxiliary port for connecting an external modem

Auxiliary connection port
HD-15 (female)
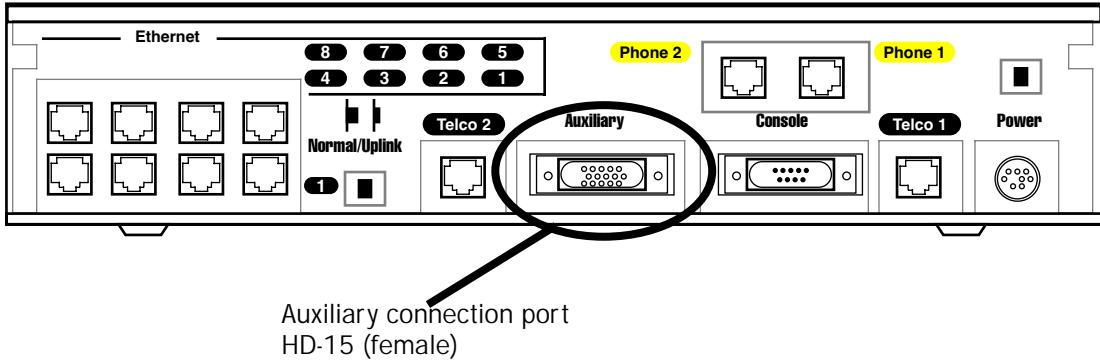
By default, the **Auxiliary** port on your Netopia R3100 is enabled for an external asynchronous modem. This means that all you have to do is connect your modem to the Auxiliary port and configure its settings in the **Line Configuration** screens under the **WAN Configuration** menu. For detailed configuration instructions see "Auxiliary Port Configuration" on page 8-10.

For pinout information on the HD-15 to DB-25 modem cable, see "Pinouts for Auxiliary Port Modem Cable," in Appendix L, "Technical Specifications and Safety Information."

Connecting to a LocalTalk network

If you have purchased the AppleTalk Kit (part number TER/ATI), you can also connect the Router to an AppleTalk network that uses either Ethernet or LocalTalk. Refer to the sheet of optional feature set add-ons in your Netopia R3100 documentation folio.

The AppleTalk feature expansion kit includes a dual RJ-11 PhoneNET® connector that attaches to the **Auxiliary** port on the Netopia R3100.

Netopia R3100 Auxiliary port for connecting to LocalTalk

Auxiliary connection port
HD-15 (female)
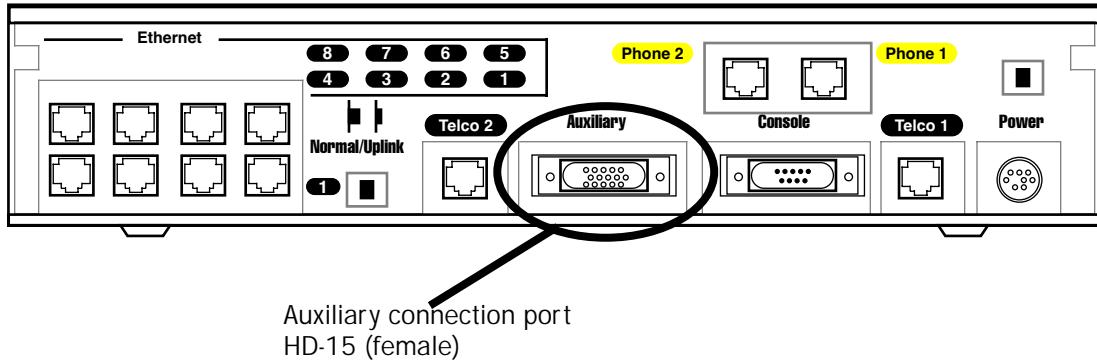
Connect the male HD-15 end of the LocalTalk cable to the **Auxiliary** port on your Netopia R3100. Connect the other end of the cable to your LocalTalk network. You can use only one connection on the Auxiliary port. You cannot use both the PhoneNET connector and an external modem.

If your LocalTalk network is not based on standard PhoneNET cabling, use a PhoneNET-to-LocalTalk adaptor cable available from Farallon. Connect the adaptor cable's RJ-11 connector to the AppleTalk cable's PhoneNet connector. Connect the cable's mini-DIN-3 connector to your LocalTalk network.

Be sure to observe the standard rules governing maximum cable lengths and limits on the number of nodes on a PhoneNET network. The dual RJ-11 PhoneNET connector allows insertion in the LocalTalk daisy chain, or at the end. If the device is connected at the end of the daisy chain, you must install the accompanying terminator.

Wiring guidelines for PhoneNET cabling

Topology	22 gauge .642 mm	24 gauge .510 mm	26 gauge .403 mm
daisy chain	n/a	n/a	1800 ft. 549 m
backbone	4500 ft. 1372 m	3000 ft. 229 m	1800 ft. 549 m
4-branch passive star*	1125 ft. 343 m	750 ft. 229 m	450 ft. 137 m
LocalTalk StarController 12-branch active star	3000 ft. 914 m	2000 ft. 610 m	1200 ft. 366 m
* distance is per branch			

Note: Make sure you *do not* connect your LocalTalk network to a Telco port or a POTS (Phone 1 and 2) port. For detailed configuration instructions see "AppleTalk Setup" on page 13-1.

Chapter 5

SmartView

This chapter discusses SmartView, the Netopia R3100's device and network web-based monitoring tool. This tool can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

Topics covered in this chapter are:

- "SmartView overview" on page 5-1
- "General Machine information page" on page 5-2
- "Connection Profiles page" on page 5-3
- "Event history pages" on page 5-3
- "Standard HTML web-based monitoring pages" on page 5-5

SmartView overview

SmartView is a Java-based applet that runs in a Web browser window. It intermittently polls the router for information to monitor the router's state and event histories. SmartView should run under any Java Virtual Machine (JVM)–enabled browser, and is therefore platform independent.

Note: The SmartView applet will only run under Java-enabled browsers. Be sure that the browser you are using is at least Microsoft Internet Explorer Version 3.0 or higher, or Netscape Navigator Version 3.0 or Communicator Version 4.0 or higher. If your browser does not meet this requirement, you can upgrade with a browser supplied on the Netopia CD.

The information you can view about your router using SmartView is shown in the table below:

Machine Information	Connection Profile Information	History Logs
Model	Profile Name	Device
Firmware version	Dial-out Profile	WAN
Ethernet IP address	Dial Number	Update
Date	Bandwidth Type	
Time	Dial Direction (In/Out)	
LED status	Remote Address	
	Gateway	
	DNS	

Machine Information	Connection Profile Information	History Logs
	DNS Alternate	
	Connect/Disconnect	

Navigating SmartView

You access the SmartView monitor by launching your web browser and entering the URL:

> http://*router_IP_Address*/smartview.html

where *router_IP_address* is the address of your router. The default address is 198.162.1.1.

Once you have invoked the SmartView pages, bookmark SmartView in your browser for easy access.

General Machine information page

SmartView uses tabbed pages to categorize information and reduce the amount of information displayed at once. Click on the tabs to display the different informational categories.

In addition to the static machine information about your router, such as model and firmware version, SmartView displays a real-time visual representation of the Netopia R3100's status lights (LEDs). This is particularly useful if the router is located out of visual range, such as in a wiring closet.
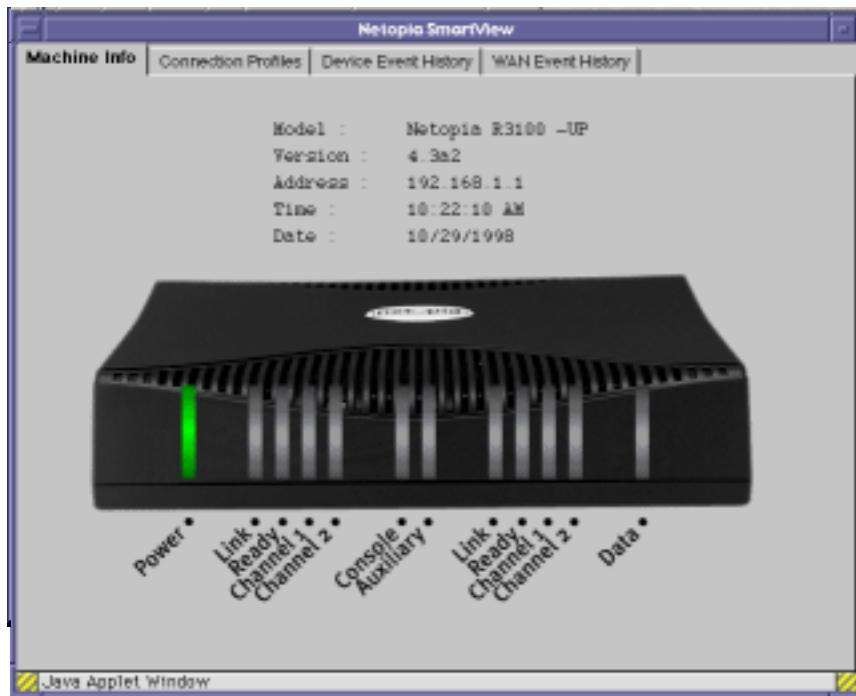
Connection Profiles page

The Connection Profiles page displays the currently active Connection Profile, and any alternate profiles you may have created. You can switch from one Connection Profile to another by disconnecting from one, and connecting to another.

- ■   To hang up the current connection, and establish the one you select, click the Disconnect button for the currently active Connection Profile.

- ■   Click the tab for the Connection Profile you want to activate.

- ■   Click the Connect Button for this Connection Profile.

Event history pages

The Netopia R3100 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R3100's built-in battery backup prevents loss of event history from a shutdown or reset.

The router's event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History pages retain records of up to 128 of the most recent events. Which events are logged is controlled by the logging function in System Configuration. See "Logging" on page 8-17.

Device Event History page

WAN Event History page

You can refresh the Event history logs by clicking the Update button.

Standard HTML web-based monitoring pages

You can also view connection profile information and event histories in the Web-based monitoring pages. These pages are provided for users without Java-enabled browsers. Unlike the SmartView pages, they are not dynamically updated.

You access the web-based monitoring pages by launching your web browser and entering the URL:

http://*router_IP_address*

where *router_IP_address* is the address of your router. The default address is 198.162.1.1.
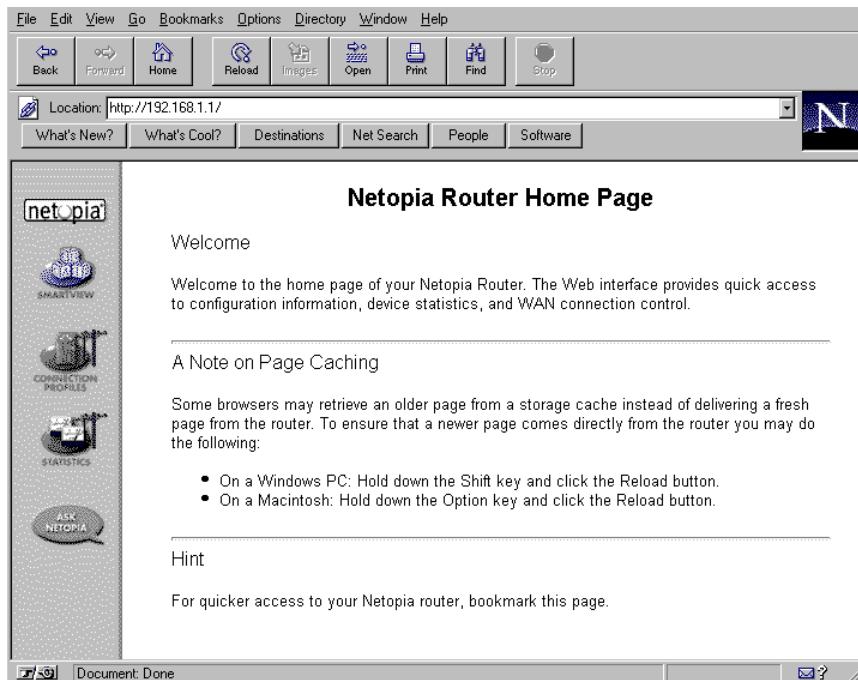
- ■ To view your connection profile information, click the **Connection Profiles** icon.

- ■ To view event histories, click the **Statistics** icon.

- ■ To go to SmartView if your browser is Java-enabled, click the **SmartView** icon.

Chapter 6

Console-based Management

This chapter describes how to use the Console-based management screens on your Netopia R3100 ISDN Router. The console screens provide an alternate method for experienced users to configure their router without using SmartStart. After completing the Easy Setup console screens, your router will be ready to connect to the Internet or another remote site.

This chapter covers the following topics:

- ■   "About Console-based Management" on page 6-1

- ■   "Connecting through a Telnet session" on page 6-2

- ■   "Connecting a local terminal console cable to your router" on page 6-3

- ■   "Navigating through the console screens" on page 6-5

About Console-based Management

Console-based management is a menu-driven interface for the capabilities built in to the Netopia R3100. Console-based management provides access to a wide variety of features that the router supports. You can customize these features for your individual setup. This section describes how to access the console-based management screens.

Console-based management screens contain seven entry points to the Netopia Router configuration and monitoring features. The entry points are displayed in the Main Menu shown below:

```
                    Netopia R3100-UP v4.3


                 Easy Setup...

                 WAN Configuration...

                 System Configuration...

                 Utilities & Diagnostics...

                 Statistics & Logs...

                 Quick Menus...

                 Quick View...
You always start from this main screen.
```
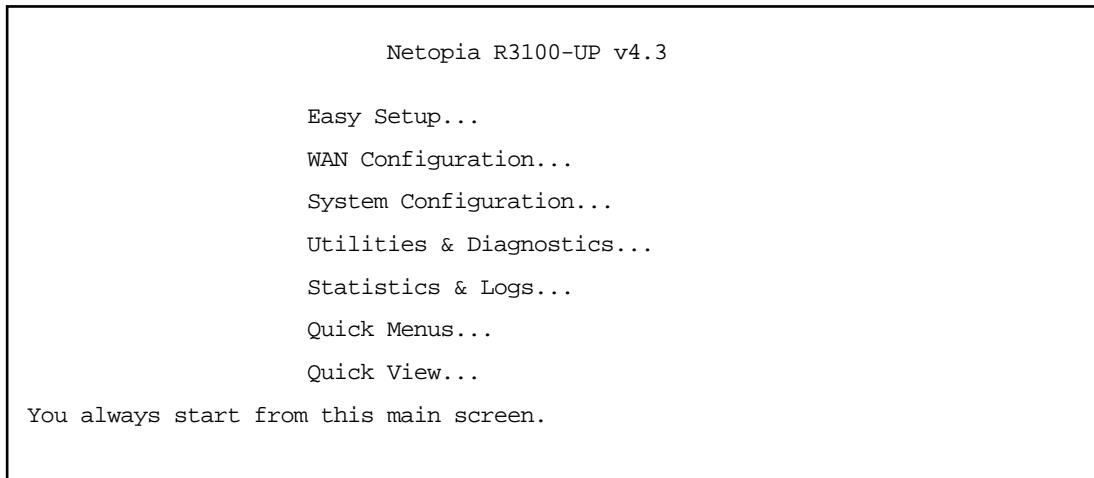
Note about screen differences. Netopia R3100 models offering different feature sets will have variations in the fields on certain screens. For example, there are switched (dial-up ISDN) and leased (Synchronous/Asynchronous, T1, and IDSL) line models, as well as models that offer feature subsets such as AppleTalk, SmartIP (Network Address Translation and DHCP) and SmartPhone (Plain Old Telephone Service). Your own console screens may look different from those illustrated in this manual.

■ The **Easy Setup** menus display and permit changing the values contained in the default Connection Profile you created when you ran the SmartStart Wizard for initial configuration. Experienced users can also use Easy Setup to initially configure the router directly through a console session without using SmartStart.

Easy Setup menus contain up to five descendant screens for viewing or altering these values. The number of screens depends on whether you have optional features installed.

■ The **WAN Configuration** menu displays and permits changing your Connection Profile(s), creating or deleting additional Connection Profiles, and configuring or reconfiguring the manner in which you may be using the router to connect to more than one service provider or remote site.

■ The **System Configuration** menus display and permit changing:

  ■ Network Protocols Setup. See "IP Setup and Network Address Translation" on page 11-1.

  ■ Filter Sets (Firewalls). See "Security" on page 15-1.

  ■ IP Address Serving. See "IP address serving" on page 11-16.

  ■ Date and Time. See "Date and Time" on page 8-14.

  ■ Console Configuration. See "Connecting a local terminal console cable to your router" on page 6-3.

  ■ SNMP (Simple Network Management Protocol). See "SNMP" on page 14-12.

  ■ Security. See "Security" on page 15-1.

  ■ Upgrade Feature Set. See "Upgrade Feature Set" on page 8-16.

  ■ Telephone Setup. See "Using SmartPhone for Telephone Services" on page 9-1.

  ■ Logging. See "Logging" on page 8-17.

■ The **Utilities & Diagnostics** menus provide a selection of seven tools for monitoring and diagnosing the router's behavior, as well as updating the firmware and rebooting the system. See "Utilities and Diagnostics" on page 16-1 for detailed information.

■ The **Statistics & Logs** menus display nine sets of tables and device logs that show information about your router, your network and their history. See "Statistics & Logs" on page 14-4 for detailed information.

■ The **Quick Menus** screen is a shortcut entry point to many of the most commonly used configuration menus that are accessed through the other menu entry points.

■ The **Quick View** menu displays at a glance current real-time operating information about your router. See "Quick View status overview" on page 14-1 for detailed information.

Connecting through a Telnet session

Features of the Netopia R3100 may be configured through the console screens.

Before you can access the console screens through Telnet, you must have:

■   a network connection locally to the router or IP access to the router through the WAN port. This could be the same connection as the one you used with SmartStart and the "Easy" path. If you used the default configuration for SmartStart, your IP address will be 192.168.1.1.

   Note: Alternatively, you can have a direct serial console cable connection using the provided console cable for your platform (PC or Macintosh) and the "Console" port on the back of the router. For more information on attaching the console cable, see "Connecting a local terminal console cable to your router," below.

■   **Telnet** software installed on the computer you will use to configure the router

Configuring Telnet software

If you are configuring your router using a Telnet session, your computer must be running a Telnet software program.

■   If you connect a PC with Microsoft Windows, you can use a Windows Telnet application or simply run Telnet from the Start menu.

■   If you connect a Macintosh computer, you can use the NCSA Telnet program supplied on the Netopia R3100 CD. You install NCSA Telnet by simply dragging the application from the CD to your hard disk.

Connecting a local terminal console cable to your router

You can perform all of the System Configuration activities for your Netopia R3100 through a local serial console connection using terminal emulation software, such as HyperTerminal provided with Windows 95 or 98 on the PC, or ZTerm, included on the Netopia CD, for the Macintosh.

The Netopia R3100 back panel has a connector labeled "Console" for attaching the Router to either a PC or Macintosh computer via the serial port on the computer. (On a Macintosh, the serial port is called the Modem port or the Printer port.) This connection lets you use the computer to configure and monitor the Netopia R3100 via the console screens.
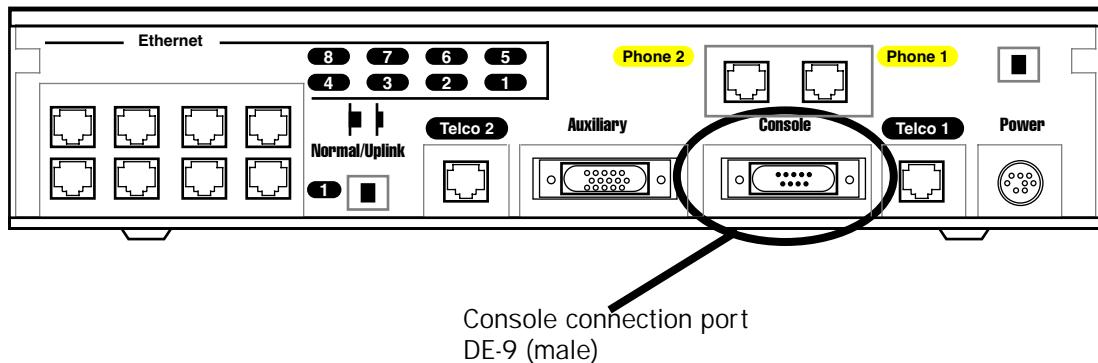
Console connection port
DE-9 (male)

To connect the Netopia R3100 to your computer for serial console communication, use the supplied dual console cable connector end appropriate to your platform:

■   one DE-9 connector end attaches to a PC

■   the mini-DIN8 connector end attaches to a Macintosh

■   the DE-9 end of the Console cable attaches to the Netopia R3100's Console port

If you are configuring your router via a *terminal* session, your computer must be running a standard terminal emulation or communications software program, such as those used with modems.

■   If you connect a PC with Microsoft Windows 95 or NT, you can use the HyperTerminal application bundled with the operating system.

■   If you connect a Macintosh computer, you can use the ZTerm terminal emulation program on the supplied Netopia R3100 CD.

Launch your terminal emulation software and configure the communications software for the following values. These are the default communication parameters that the Netopia R3100 uses.

Parameter	Suggested Value
Terminal type	**PC**: ANSI-BBS **Mac**: ANSI, VT-100, or VT-200
Data bits	8
Parity	None
Stop bits	1
Speed	Options are: 9600, 19200, 38400, or 57600 bits per second
Flow Control	None
Note: The router firmware contains an autobaud detection feature. If you are at any screen on the serial console, you can change your baud rate and press Return (HyperTerminal for the PC requires a disconnect). The new baud rate is displayed at the bottom of the screen.	

Navigating through the console screens

Use your keyboard to navigate the Netopia R3100's configuration screens, enter and edit information, and make choices. The following table lists the keys to use to navigate through the console screens.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
To set a change to a selected item or open a pop-up menu of options for a selected item like entering an upgrade key	Return or Enter
Change a toggle value (Yes/No, On/Off)	Tab
Restore an entry or toggle value to its previous value	Esc
Move one item up	Up arrow or Control + k
Move one item down	Down arrow or Control + j
Display a dump of the device event log	Control + e
Display a dump of the WAN event log	Control + f
Refresh the screen	Control + L
Go to topmost selectable item	<
Go to bottom right selectable item	>

To help you find your way to particular screens, some sections in this guide begin with a graphical path guide similar to the following example:

```
┌──────────┐      ┌──────────────┐      ┌──────────────────┐      ┌──────────┐
│  Main    │─────▶│   System     │─────▶│ Network Protocols│─────▶│ IP Setup │
│  Menu    │      │Configuration │      │     Setup        │      │          │
└──────────┘      └──────────────┘      └──────────────────┘      └──────────┘
```
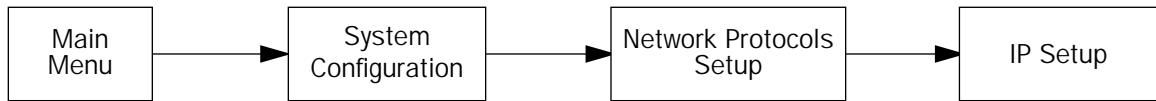
This particular path guide shows how to get to the Network Protocols Setup screens. The path guide represents these steps:

1.   Beginning in the Main Menu, select the **System Configuration** item and press Return.

2.   Select the **Network Protocols** item in the System Configuration screen and press Return.

3.   Select the **IP Setup** item in the Network Protocols Setup screen and press Return.

To go back in this sequence of screens, use the Escape key.

Chapter 7

Easy Setup

This chapter describes how to use the Easy Setup console screens on your Netopia R3100 ISDN Router. The Easy Setup console screens provide an alternate method for experienced users to set up their router's Connection Profiles without using SmartStart. After completing the Easy Setup console screens, your router will be ready to connect to the Internet or another remote site.

This chapter covers the following topics:

■ "Easy Setup console screens" on page 7-1

■ "Beginning Easy Setup" on page 7-3

■ "Configuring Frame Relay" on page 7-11

Easy Setup console screens

Using four Easy Setup console screens, you can:

■ set up your switch type and datalink parameters

■ create or modify a Connection Profile for your Router for the connection to your ISP or remote location

■ set up IP addresses and IP address serving

■ password protect configuration access to your Netopia R3100 ISDN Router

How to access the Easy Setup console screens

To access the console screens, Telnet to the Netopia Router over your Ethernet network, or you can physically connect with a serial console cable and access the Netopia Router with a terminal emulation program. See "Connecting through a Telnet session" on page 6-2 or "Connecting a local terminal console cable to your router" on page 6-3.

Note: Before continuing, make sure that you have the information that your telephone service provider, ISP, or network administrator has given you to configure the Netopia Router.

The Netopia Router's first console screen, Main Menu, appears in the terminal emulation window of the attached PC or Macintosh when:

■ the Netopia Router is turned on

■ the computer is connected to the Netopia Router

■ the Telnet or terminal emulation software is running and configured correctly.

A screen similar to the following appears:

```
                        Netopia R3100-UP v4.3

                 Easy Setup...

                 WAN Configuration...

                 System Configuration...

                 Utilities & Diagnostics...

                 Statistics & Logs...

                 Quick Menus...

                 Quick View...




   Return/Enter goes to Easy Setup -- minimal configuration.
   You always start from this main screen.
```
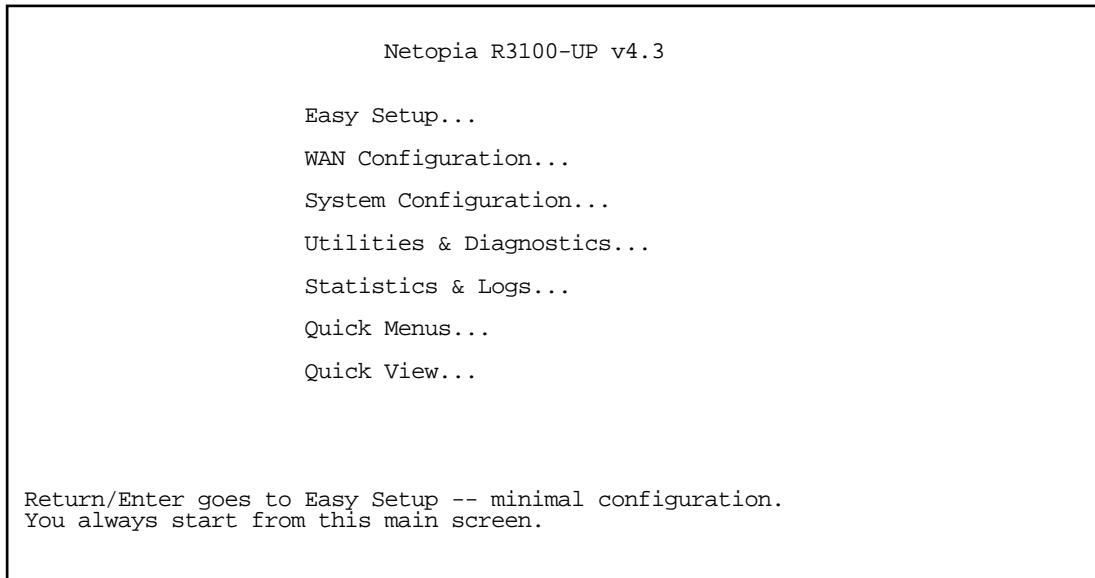
If you do not see the Main Menu, verify that:

■   the computer used to view the console screen has its serial port connected to the Netopia R3100's "Console" port or an Ethernet connection to one of its Ethernet ports. See "Connecting a local terminal console cable to your router" on page 6-3 or "Connecting through a Telnet session" on page 6-2.

■   the Telnet or terminal emulation software is configured for the recommended values.

■   if you are connecting via the Console port, the console's serial port is not being used by another device, such as an internal modem, or an application. Turn off all other programs (other than your terminal emulation program) that may be interfering with your access to the port.

■   you have entered the correct password, if necessary. Your Netopia R3100's console access may be password protected from a previous configuration. See your system administrator to obtain the password.

   See Appendix A, "Troubleshooting," for more suggestions.

Beginning Easy Setup

To begin Easy Setup, select **Easy Setup** in the Main Menu, then press Return.

The Easy Setup screen appears. For an IDSL router, skip to "IDSL Easy Setup" on page 7-6.

```
                         ISDN Easy Setup

        Circuit Type...                  ISDN, Switched
        Switch Type...                   National ISDN-1 (NI-1) Detected

        Directory Number 1:              5088324614          Detected
        Directory Number 2:              5088324615          Detected
        SPID 1:                          50883246141         Pass
        SPID 2:                          50883246152         Pass

        PBX Prefix:

        Data Link Encapsulation...       PPP




        TO MAIN MENU                     NEXT SCREEN

Return/Enter to select <among/between> ...
Enter information supplied to you by your ISDN phone company.
```

ISDN Easy Setup

Note: The ISDN Wizard is designed to automatically detect and configure most of your ISDN parameters for you, without your having to enter anything except a PBX dialing prefix, if you need one. The steps described in this section allow you to either accept the detected values or override them in a manual mode if you want to. As soon as the router is physically connected to the ISDN line and powered on, it tries to detect the switch type, directory numbers, and SPIDs. If it is successful, the screen above will be displayed with all the fields already filled in, except the PBX Prefix field.

The Easy Setup Profile screen is where you configure the parameters that control the Netopia R3100's connection to a specific remote destination, usually an ISP or a corporate site.

On a Netopia R3100 ISDN Router you can add up to 15 more connection profiles, for a total of 16.

1. Select **Circuit Type** and press Return. From the pop-up menu, select:

    ISDN, Switched if you have a switched ISDN line. This option covers the broadest range of U and ST applications, and enables the ISDN Wizard automatic switch type and SPID detection for U interfaces and defaults to Euro-ISDN for ST models, or

    ISDN, Leased if you have a dedicated or leased ("nailed-up") ISDN line that uses a single B channel (64K), 2B (128K), or the entire ISDN bandwidth of 2B+D (144K), or

    IDSL, Ascend if your leased line service provider uses Ascend equipment (only available on U interfaces), or

IDSL, CMN if your leased line service provider uses Copper Mountain equipment (this is the default for model R3100-I)

Note: The Switch Type, SPIDs, and Directory Numbers apply only to Switched ISDN service. If you select either IDSL option, these fields are not displayed.

If you select ISDN, Leased as your circuit type, select **Data Rate (kbps)**. From the pop-up menu, select the appropriate B-channel, such as B1, B2, B1+B2, or 2B+D. Then skip to step 8.

It is possible to configure the router for any available circuit type: **ISDN, Switched**, **ISDN, Leased**, **IDSL, Ascend**, or **IDSL, CMN**, depending on the switch gear you are connected to.

Netopia Model	Default Circuit Type	Default Datalink Encapsulation	Alternate Datalink Encapsulation
R3100-S and SP	ISDN, Switched (default)	PPP	Frame Relay, HDLC
	ISDN, Leased	PPP	Frame Relay, HDLC
	IDSL, Ascend	PPP	None
	IDSL, CMN	Frame Relay	ATM FUNI
R3100-U and UP	ISDN, Switched (default)	PPP	Frame Relay, HDLC
	ISDN, Leased	PPP	Frame Relay, HDLC
	IDSL, Ascend	PPP	None
	IDSL, CMN	Frame Relay	ATM FUNI
R3100-I	IDSL, CMN (default)	Frame Relay	ATM FUNI
	ISDN, Switched	PPP	Frame Relay, HDLC
	ISDN, Leased	PPP	Frame Relay, HDLC
	IDSL, Ascend	PPP	None

If you create a connection profile using a particular datalink encapsulation method, that profile will take precedence whenever you connect to a line that uses that datalink encapsulation. If there is no connection profile with the datalink encapsulation method that the line uses, the router will default to using the default profile. See "The Default Profile" on page 8-6 for more information.

2. Select **Switch Type** and press Return. From the pop-up menu, select the switch protocol your ISDN service provider uses.

North American options are:

■ **Auto-Detect** (the default): using this feature, the router will attempt to detect what type of switch you are connecting to, what your directory numbers and SPIDs are, and configure itself accordingly.

If you select Auto-Detect from the popup menu, you may see the following screen if the router has not

already detected the switch type automatically. If you know your switch type, you can choose CANCEL and select one of the other options manually. If the switch type has already been detected, the screen (as shown on page 7-3) will so indicate. If the switch type has not been detected, the screen will indicate "Failed," and you should select it manually from the other available options in the popup menu.

```
+----------------------------------------------------------------+
+----------------------------------------------------------------+
|                                                                |
|  Attempting to determine Switch Type.  This may take awhile.   |
|  If you want to proceed with manual configuration hit 'CANCEL'.|
|                                                                |
|  Status: Detecting Switch Type                                 |
|                                                                |
|                         CANCEL                                 |
|                                                                |
+----------------------------------------------------------------+
```
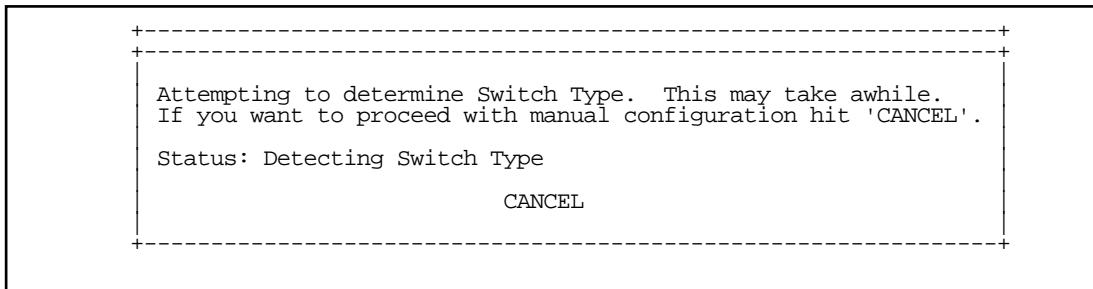
- ■ **National ISDN-1 (NI-1)**

- ■ **AT&T 5ESS Pt-to-Pt**

- ■ **AT&T 5ESS Multipoint**

- ■ **Nortel DMS100 Custom**

European models: For European countries other than the United Kingdom, use the **EuroISDN/ETSI** setting. United Kingdom users select **United Kingdom - EuroISDN**.

3. Select **Directory Number 1.**

   The router attempted to detect your Directory Number(s) when you selected Auto-Detect in Step 1.

   If it succeeded, the directory number(s) will be displayed, and the screen will indicate "Detected" (as shown on page 7-3).

   If it failed to detect your directory numbers, the fields will remain blank, and you must enter the primary directory number as you would dial it, including area code. Do not enter access prefixes such as Centrex or PBX prefixes like "9" (for an outside line). Press Return.

4. If you have a second directory number, select **Directory Number 2** and enter the secondary directory number as you would dial it, including area code. Press Return.

   When you enter your directory number(s), the router will attempt to determine appropriate SPID numbers for your connection. The following screen appears.

```
+----------------------------------------------------------------+
+----------------------------------------------------------------+
|                                                                |
|  Attempting to determine SPID.  This may take awhile.          |
|  If you want to proceed with manual configuration hit 'CANCEL'.|
|                                                                |
|  Status: Detecting SPID                                        |
|                                                                |
|                         CANCEL                                 |
|                                                                |
+----------------------------------------------------------------+
```
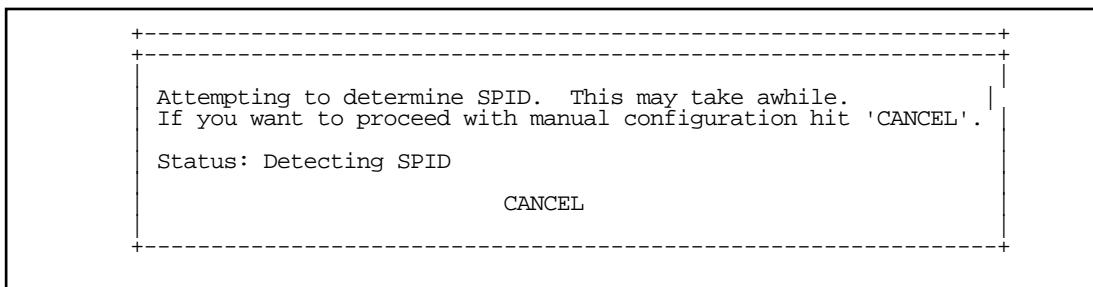
If the router detected your SPIDs successfully, the screen (as shown on page 7-3) displays them and indicates "Pass," meaning that the entered SPIDs initialized. If the SPIDs are entered incorrectly, the fields will remain blank and the screen will indicate "Fail." You must then re-enter them manually.

5. **U models:** Select **SPID 1** and enter the primary SPID number. If you did not receive a SPID (AT&T 5ESS custom point-to-point switches have no SPID), you should skip this and the following step.

   Note: SPIDS and DNs may be entered with or without parentheses, commas, or dashes, as you are accustomed to writing them.

6. **U models:** If you have a second SPID, select **SPID 2** and enter the secondary SPID number.

   Note: SPID1 and **SPID2** are not displayed for switch types outside North America.

7. If you require a dialing prefix such as "9" to access an outside line on a PBX or Centrex phone system, select **PBX Prefix** and enter your dialing prefix. Press Return.

8. Select **Data Link Encapsulation** and highlight the method of encapsulation that you want to use from the pop-up menu. The choices offered are PPP, HDLC, or Frame Relay. The default for switched interfaces is PPP. Press Return.

   Note: If you select Frame Relay as your Datalink Encapsulation method, see "Configuring Frame Relay" on page 7-11 for additional options and detailed instructions.

9. Select **NEXT SCREEN** and press Return. The "Easy Setup Profile" screen (shown on page 7-7) appears.

Any changes you make to the ISDN configuration now or in the future will take effect immediately. You do not have to restart the router.

IDSL Easy Setup

The Easy Setup screen for an R3100-I IDSL router is different from the ISDN Easy Setup screen.

```
                        ISDN Easy Setup


        Circuit Type...                 IDSL, CMN




                                     +-------------+
                                     +-------------+
        Data Link Encapsulation...   | Frame Relay |
                                     | ATM FUNI    |
                                     +-------------+


        TO MAIN MENU                    NEXT SCREEN


```
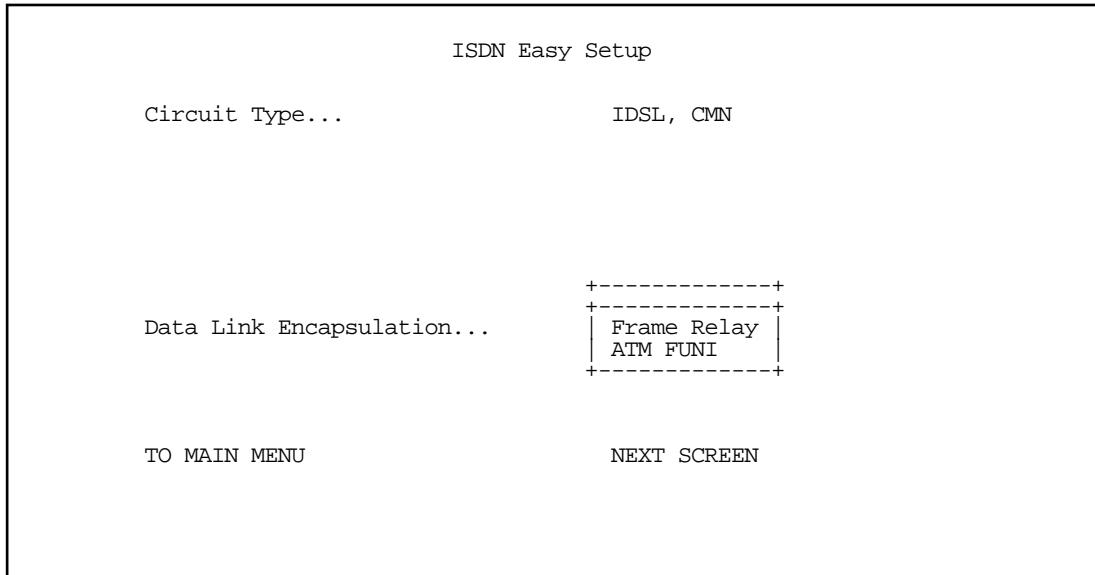
Choose your Data Link Encapsulation method. Frame Relay is the default. The choice of Frame relay or ATM FUNI depends information supplied to you by your DSL service provider.

Easy Setup Profile

The Easy Setup Connection Profile screen is where you configure the parameters that control the ISDN Netopia Router's connection to a specific remote destination, usually another network.

```
                       Connection Profile 1: Easy Setup Profile


        Number to Dial:

        Address Translation Enabled:       Yes


        Local WAN IP Address:              0.0.0.0

        Remote IP Address:                 127.0.0.2
        Remote IP Mask:                    255.0.0.0

        PPP Authentication...              PAP
        Send User Name:
        Send Password:


        PREVIOUS SCREEN                    NEXT SCREEN

   Enter the directory number for the remote network connection.
   Enter basic information about your WAN connection with this screen.
```

1. Select **Number to Dial** and enter the ISDN telephone number you received from your ISP. This is the number the Netopia R3100 dials to reach your ISP. Enter the number as you would dial it, including any required prefixes (such as area, access, and long-distance dialing codes).

   If you selected ISDN, Leased, or either of the IDSL options, as your router's Circuit Type in the ISDN Easy Setup screen or if you have an IDSL router, Number to Dial will not be an available option. Other differences include Frame Relay Management Type. For information on Frame Relay Management Type see "Configuring Frame Relay" on page 7-11. Frame Relay is an alternative datalink encapsulation method for use over unswitched connections. If this does not apply to your connection, you can skip the corresponding sections.

2. To enable address translation, toggle **Address Translation Enabled** to **Yes**. For more information on Network Address Translation, see Chapter 11, "IP Setup and Network Address Translation."

   Then select the **Local WAN IP Address** field. The default address is 0.0.0.0, which allows for dynamic addressing, your ISP assigning an address each time you connect. However, you may enter another address if you want to use static addressing.

   Note: When using HDLC datalink encapsulation and Network Address Translation, you must use a static address.

3. If your ISP uses Numbered (Interface-based Routing), select **Local WAN IP Address** and enter the local WAN address your ISP gave you.

When using numbered interfaces, the Netopia Router will use its local WAN IP address and subnet mask to send packets to the remote router. Both routers have WAN IP addresses and subnet masks associated with the connection.

If your ISP uses Unnumbered (System-based Routing) or your datalink encapsulation is not Frame Relay, select **Remote IP Address** and enter the IP address your ISP gave you. Then select **Remote IP Mask** and enter the IP subnet mask of the remote site you will connect to.

When using unnumbered interfaces, the Netopia Router will use either its local Ethernet IP address or its NAT address (if so configured) and subnet mask to send packets to the remote router. Neither router has a WAN IP address or subnet mask associated with this connection.

Note: If your ISP has not given you their IP or subnet mask addresses, then you may enter an IP address such as 127.0.0.2, and an IP subnet mask such as 255.0.0.0. which are acceptable as defaults values, and will typically be assigned at the time of connection.

4. **For circuits with PPP enabled:** Select the **PPP Authentication** pop-up menu and choose the type of connection security your ISP told you to use (either **None**, **PAP**, **CHAP**, **PAP-TOKEN**, or **CACHE-TOKEN**). If you choose **PAP**, **CHAP**, **PAP-TOKEN**, or **CACHE-TOKEN**, go to the next step. If your ISP does not use any of these authentication methods, choose **None** and skip to the last step. When you create a connection profile from Easy Setup, the default setting is PAP.

5. **For circuits with PPP enabled:** If your ISP uses PAP, select **Send User Name** and enter the user name your ISP gave you to connect. Then select **Send Password** and enter the password.

   If your ISP uses CHAP, select **Send Host Name** and enter the user name your ISP gave you to connect. Then select **Send Secret** and enter the secret (CHAP term for password) your ISP gave you.

6. Select **NEXT SCREEN** and press Return. The IP Easy Setup screen appears.

IP Easy Setup

The IP Easy Setup screen is where you enter information about your Netopia Router's:

■   IP address

■   Subnet mask

■   Default gateway IP address

■   Domain name server IP address

■   IP address serving information, such as the number of client IP addresses and the 1st client address; and

You should consult with your network administrator to obtain the information you will need. For more information about setting up IP, see "IP Setup and Network Address Translation" on page 11-1.

```
                          IP Easy Setup


          Ethernet IP Address:            192.168.1.1
          Ethernet Subnet Mask:           255.255.255.0

          Domain Name:
          Primary Domain Name Server:     192.168.1.10
          Secondary Domain Name Server:   0.0.0.0

          Default IP Gateway:             0.0.0.0

          IP Address Serving:             On

          Number of Client IP Addresses:  100
          1st Client Address:             192.168.1.3



          PREVIOUS SCREEN                  NEXT SCREEN

   Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
   Set up the basic IP & IPX attributes of your Netopia in this screen.
```

1.   Select **Ethernet IP Address** and enter the first IP address from the IP address range your ISP has given you. This will be the Netopia Router's IP address.

   If Network Address Translation is enabled in the Easy Setup connection profile, the Ethernet IP Address defaults to an address within a range reserved by the Internet address administration authority for use within private networks, 192.168.1.1.

   Because this is a private network address, it should never be directly connected to the Internet. Using NAT for all your connection profiles will ensure this restriction. See "IP Setup and Network Address Translation" on page 11-1 of this guide for more information.

2.   Select **Ethernet Subnet Mask** and enter the subnet mask your ISP has given you. The **Ethernet Subnet Mask** defaults to a standard class C mask, 255.255.255.0.

3.   Select **Domain Name** and enter the domain name your ISP has given you.

4.   Select **Primary Domain Name Server** and enter the IP address your ISP has given you.

5. The **Default IP Gateway** defaults to the remote IP address you entered in the Easy Setup connection profile. If the Netopia Router does not recognize the destination of any IP traffic, it forwards that traffic to this gateway – set to 127.0.0.2 if your ISP does not otherwise specify.

    Do not confuse the remote IP address and the default gateway's IP address with the block of local IP addresses you receive from your ISP. You use the local IP addresses for the Netopia R3100's Ethernet port and for IP clients on your local network. The remote IP address and the default gateway's IP address should point to your ISP's router.

6. To use DHCP and (if installed) MacIP address serving, toggle **IP Address Serving** to **On**.

    Note: For information about dynamic IP address serving, see "IP Setup and Network Address Translation" on page 11-1.

7. If **IP Address Serving** is **On**, select **Number of Client IP Addresses**. Then enter the number of available host addresses for the Netopia R3100 ISDN Router to allocate to the client computers on your network. This number defaults to the balance of the subnet addresses above the Netopia Router's address.

8. If **IP Address Serving** is **On**, select **1st Client Address** and enter the first IP address in the set of allocated served IP addresses.

    Note: On a Netopia R3100 the factory default IP Address serving settings are:

    1st Client Address: 192.168.1.3

    Number of Client IP Addresses: unlimited models:100; limited models: number of users minus 1

    (this allows for one static address at 192.168.1.2 for the server)

    The values you set in this screen are displayed in the "Quick View status overview" shown on page 14-2.

9. Press Return. The Easy Setup Security Configuration screen appears.

Easy Setup Security

The Easy Setup Security Configuration screen lets you password-protect your Netopia R3100. Input your Write Access Name and Write Access Password with names or numbers totaling up to eleven digits.

If you password protect the console screens, you will be prompted to enter the name and password you have specified every time you log in to the console screens. Do not forget your name and password. If you do, you will be unable to access any of the configuration screens.

Additional security features are available. See "Security" on page 15-1.

```
                    Easy Setup Security Configuration


It is strongly suggested that you password-protect configuration access to your
Netopia. By entering a Name and Password pair here, access via serial, PC Card,
Telnet, SNMP and Web Server will be password-protected.

Be sure to remember what you have typed here, because you will be prompted for
it each time you configure this Netopia.



        Write Access Name:

        Write Access Password:




        PREVIOUS SCREEN        TO MAIN MENU       RESTART DEVICE


Configure a Configuration Access Name and Password here.
```

The final step in configuring the Easy Setup console screens is to restart the Netopia R3100, so the configuration settings take effect.

1. Select **RESTART DEVICE**. A prompt asks you to confirm your choice.

2. Select **CONTINUE** to restart the Netopia Router and have your selections take effect.

Note: You can also restart the system at any time by using the restart utility (see "Restarting the system" on page 16-12) or by turning the Netopia Router off and on with the power switch.

Easy Setup is now complete.

Configuring Frame Relay

Frame Relay is an alternative datalink encapsulation method for use over unswitched connections. If this does not apply to your connection, you can skip the corresponding sections.

You can specify Frame relay as your Datalink Encapsulation method in either of two ways:

■   the "Easy Setup Frame Relay screens" on page 7-12 or

■   the "WAN Configuration Frame Relay screens" on page 7-13

Easy Setup Frame Relay screens

```
+-----------+        +-----------+        +-----------+
|   Main    |  ───►  |   Easy    |  ───►  |   ISDN    |
|   Menu    |        |   Setup   |        | Easy Setup|
+-----------+        +-----------+        +-----------+
```

```
                        ISDN Easy Setup


           Circuit Type...                  Switched
           Switch Type...                   EuroISDN/ETSI



           Directory Number 1:              5105776430
           Directory Number 2:              5105776431

           PBX Prefix:                   +-------------+
                                         +-------------+
           Data Link Encapsulation...    | PPP         |
                                         | HDLC        |
                                         | Frame Relay |
                                         +-------------+

           TO MAIN MENU                     NEXT SCREEN
```

For IDSL routers, Frame Relay encapsulation is the default.

```
                        IDSL Easy Setup

                                         +-------------+
                                         +-------------+
           Data Link Encapsulation...    | Frame Relay |
                                         | ATM FUNI    |
                                         +-------------+







            TO MAIN MENU                    NEXT SCREEN

     Return/Enter goes to new screen.
     Enter information supplied to you by your ISDN phone company.
```

WAN Configuration Frame Relay screens

The ISDN Line Configuration menu also offers the options of either PPP, HDLC, or Frame Relay as your datalink encapsulation method.

```
+--------+       +---------------+       +---------+       +---------------+
|  Main  |       |     WAN       |       |   WAN   |       |   ISDN Line   |
|  Menu  | ====> | Configuration | ====> |  Setup  | ====> | Configuration |
+--------+       +---------------+       +---------+       +---------------+
```

```
                        ISDN Line Configuration


            Circuit Type...                 Switched
            Switch Type...                  EuroISDN/ETSI



            Directory Number 1:             5105776430
            Directory Number 2:             5105776431

            PBX Prefix:                    +-------------+
                                           +-------------+
            Data Link Encapsulation...     | PPP         |
                                           | HDLC        |
                                           | Frame Relay |
                                           +-------------+

```

For IDSL routers, Frame Relay is the default.

```
                        IDSL Line Configuration



            Data Link Encapsulation...       Frame Relay







            Aux Serial Port...               LocalTalk




     Enter information supplied to you by your ISDN phone company.
```

Frame Relay configuration

If you chose Frame Relay as your datalink encapsulation type you can now configure the Frame Relay options.

```
                         WAN Configuration

                 WAN (Wide Area Network) Setup...

                 Display/Change Connection Profile...
                 Add Connection Profile...
                 Delete Connection Profile...

                 Default Answer Profile...

                 Scheduled Connections...

                 Frame Relay Configuration...
                 Frame Relay DLCI Configuration...

                 Establish WAN Connection...
                 Disconnect WAN Connection...



     Return/Enter for WAN line configuration.
     From here you will configure yours and the remote sites' WAN information.
```

From the WAN Configuration screen, select **WAN Setup**, then select the **Frame Relay Configuration** option and press Return. The Frame Relay Configuration screen appears.

```
                      Frame Relay Configuration

         LMI Type...                      ANSI (Annex D)
         T391 (Polling Interval in secs): 10
         N391 (Polls/Full Status Cycles): 6
         N392 (Error Threshold):          3
         N393 (Monitored Event Window):   4

         Tx Injection Management...       Standard
         Default CIR:                     64000
         Default Bc:                      64000
         Default Be:                      0

         Congestion Management Enabled:   No



         Maximum Tx Frame Size:           1520


     Return/Enter goes to new screen.
     Enter Information supplied to you by your telephone company.
```

Note: The default configuration for the model R3100-I is **No LMI** as an LMI Type and DLCI 16 is statically configured. This is appropriate for current versions of the Copper Mountain DSLAM firmware. Future versions of the Copper Mountain firmware may support multiple statically configured DLCIs or DLCIs other than 16, or an LMI setting other than No LMI. In that case there may be no need to statically configure DLCIs at all since the router may be able to detect what DLCIs are configured between it and the DSLAM. Consult your service provider, CE200 documentation, or technical notes from Copper Mountain for DSLAM configuration.

The following configuration information is provided for options available in future versions of the Copper Mountain firmware.

1. Select **LMI Type** (Link Management Type) and press Return. From the pop-up menu, highlight either **ANSI (Annex D)**, **CCITT (Annex A)**, **LMI**, or **No LMI**. The default is **No LMI**. Press Return.

    See *"Frame Relay DLCI configuration" on page 7-16* for instructions.

    Specifying the Link Management Type is the first step in configuring Frame Relay.

    ■   If you select an LMI Type (Link Management Type) other than None, the **T391** option specifies the number of seconds between the Status Enquiry messages. The default setting is 10.

    ■   The **N391** option specifies the frequency of full status polls, in increments of the basic (T391) polling cycle. The default setting is 6.

    ■   The **N392** option specifies the maximum number of (link reliability, protocol, and sequence number) error events that can occur within the N393 sliding window. If an N392 threshold is exceeded, the switch declares the Netopia Router inactive. The default setting is 3.

    ■   The **N393** option allows the user to specify the width of the sliding N392 monitored event window. The default setting is 4.

2. Select **Tx Injection Management** and press Return. From the pop-up menu, highlight **Standard** if you want the frames on your line that exceed the configured service parameters to be dropped at the router, **Buffered** if you want the frames on your line that exceed the link capacity to be delayed until the link is less busy, or **None** if you want all of the frames on your line to be transmitted. Press Return.

    Note: If you select **None** as the Tx Injection Management type, the three Tx Injection Management options listed below will remain hidden. Go to step 4.

    If you select **Standard** or **Buffered** as the Tx Injection Management type, then the **Default CIR**, **Bc**, and **Be** values will appear (in the corresponding fields below the Tx Injection Management field) in order for you to define the parameters the management algorithm.

    ■   The **Default CIR** (CIR also referred to as Committed Information Rate) represents the average capacity available to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). This setting defaults to 64000, but you may modify the capacity rate if this setting will not be applicable to you.

    ■   The **Default Bc** (Bc also referred to as Committed Burst Size) represents the maximum amount of data that your Frame Relay service provider agrees to transfer from a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). This setting defaults to 64000, but you may change the capacity rate if this setting needs to be modified.

    ■   The **Default Be** (Be also referred to as Excess Burst Size) represents the maximum amount of data that your Frame Relay service provider will attempt to deliver to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). This setting defaults to 0, but you may change the capacity rate if this setting needs to be modified.

Note: Some Frame Relay service providers allow for over-subscription of the DLCIs, which occurs when the total number of CIRs for all PVCs exceeds the line rate setup.

3. Select **Congestion Management Enabled** and toggle to **Yes** or **No** depending on whether you use this selection. Press Return.

    If Congestion Management is enabled, this option causes the Netopia Router to use in-bound FECNs (Forward Explicit Congestion Notification). This feature is designed to notify you that congestion avoidance procedures should be initiated where applicable for traffic in the same direction as the received frame. It indicates that the frame in question, has encountered congested resources.

    Note: The Congestion Management Enabled field will only appear if Standard or Buffered is selected as the option from the Tx Injection Management field.

4. Select **Maximum Tx Frame Size** and press Return. The default is automatically set to a value suitable for encapsulating a full ethernet packet's transmission load, however you may change the Maximum Frame Size to suit your networks transmission load. Press Return.

You are now done configuring the Frame Relay Configuration screen. Press the Escape key to return to the WAN Configuration screen. If you need to configure your DLCIs, go to the next section.

Frame Relay DLCI configuration

If you selected **None** as your LMI Type then you will need to manually configure your DLCIs.

A Frame Relay DLCI is a set of parameters that tells the Netopia Router how to initially connect to a remote destination.

The Netopia Router supports up to 16 different Frame Relay DLCI profiles.

Each Frame Relay DLCI configuration you set up allows the Netopia Router to connect your network to another network that uses IP or IPX over Frame Relay.

To go to the Frame Relay DLCI configuration screen, select **Frame Relay DLCI Configuration** in the WAN Configuration screen.

```
                     Frame Relay DLCI Configuration

                            Display/Change DLCIs...

                            Add DLCI...

                            Delete DLCI...






      Add, delete, and modify DLCIs from here.
```
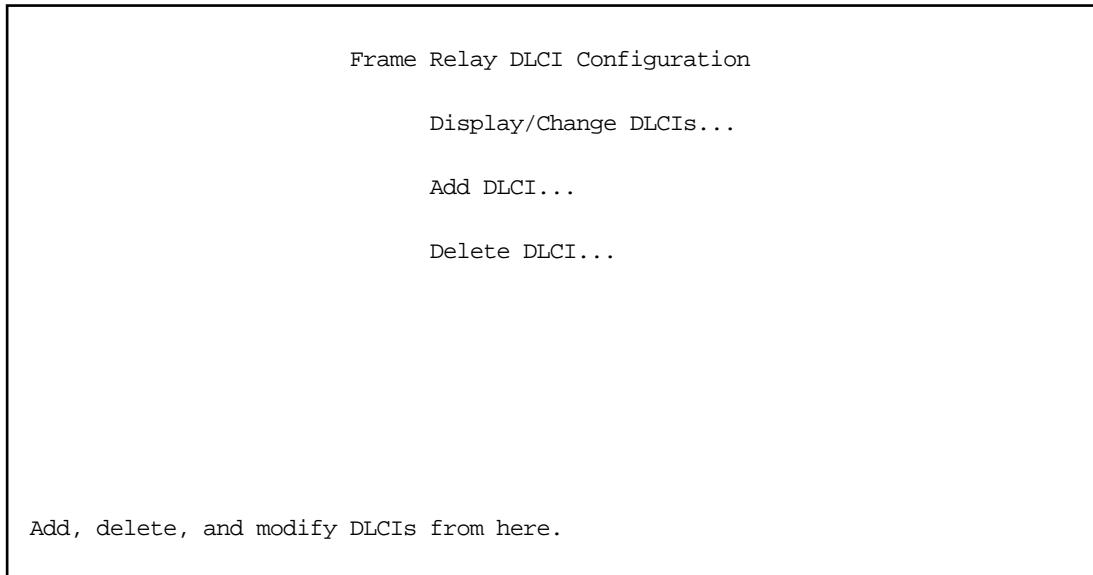
Displaying a Frame Relay DLCI configuration table

To display a view-only table of the Frame Relay DLCIs, select **Display/Change DLCIs** in the Frame Relay DLCI Configuration screen, and press Return.

The Frame Relay DLCI Configuration table is a handy way to quickly view the DLCI names and DLCI numbers that you attribute to your Frame Relay profiles.

```
                   Frame Relay DLCI Configuration
                 +-DLCI Name----------DLCI Number-+
                 +-------------------------------+
                 |                                |
                 | DLCI 16                    16  |
                 |                                |
                 |                                |
                 |                                |
                 |                                |
                 |                                |
                 |                                |
                 |                                |
                 |                                |
                 |                                |
                 +-------------------------------+

      Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

Changing a Frame Relay DLCI configuration

To modify a Frame Relay DLCI configuration, select **Display/Change DLCIs** in the Frame Relay DLCI Configuration screen.

Select a DLCI Name from the table and press Return to go to the **Change DLCI** screen. The parameters in this screen are the same as the parameters in the Add DLCI screen. To find out how to set them, see "Adding a Frame Relay DLCI configuration" on page 7-19.

```
                        Change DLCI
        DLCI Name:                      DLCI 33

        DLCI Enabled:                   Yes

        DLCI Number (16-991):           32

        Remote IP Address:              2.0.0.2
```

Adding a Frame Relay DLCI configuration

To add a new Frame Relay DLCI, select **Add DLCI** in the Frame Relay DLCI Configuration screen and press Return. The Add DLCI screen appears.

```
                            Add DLCI


         DLCI Name:                       DLCI 16

         DLCI Enabled:                    Yes

         DLCI Number (16-991):            16


         Remote IP Address:               0.0.0.0

         Data Flow Parameters--------------Use Default---------Value----
         CIR:                             Yes
         Bc:                              Yes
         Be:                              Yes



         ADD DLCI NOW                     CANCEL

    Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
    Here you configure the parameters for a single DLCI (Data Link Circuit ID).
```

1. Select **DLCI Name** and enter a name for this individual Frame Relay DLCI profile. It can be any name you wish. For example: the name of your ISP or remote branch your connecting to such as the corporate headquarters of your company.

    Note: The Netopia Router allows Frame Relay DLCIs to be named, so that you can easily reference and differentiate them. This is accomplished by giving a **DLCI Name** to a **DLCI Number**.

2. Select **DLCI Enabled** and toggle it to **Yes** to activate the profile. If you disable this profile, the Netopia Router will automatically disable and block access to a specific remote DLCI.

3. Select **DLCI Number (16-991)** and enter a number for this individual DLCI. Check with your Frame Relay provider to find out what numbers are allocated for each of your DLCI profiles. The DLCI number range should fall within the range of 16-991.

4. Select **Remote IP Address** and enter the remote IP address your ISP or network administrator gave you that represents the remote sites IP address for their router. Press Return.

If you select **Standard** or **Buffered** as the Tx Injection Management type in the Frame Relay Configuration screen go to the next bulleted item below. If you selected **None** in the Frame Relay Configuration screen go to step 6.

    Below the Remote IP Address field, the following Data Flow Parameters appear:

    ■ The **CIR** (Committed Information Rate) represents the average capacity available to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). The setting defaults to 64000, but you may modify the capacity rate by toggling the selection in the **Use Default** field to **No**. You can then enter a different capacity rate in the **Value** field.

    ■ The **Bc** (Committed Burst Size) represents the maximum amount of data that your Frame Relay service provider agrees to transfer from a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection

Identifier). The setting defaults to 64000, but you may modify the committed burst size by toggling the selection in the **Use Default** field to **No**. You can then enter a different committed burst size in the **Value** field.

■   The **Be** (Excess Burst Size) represents the maximum amount of data that your Frame Relay service provider will attempt to deliver to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). The setting defaults to 0, but you may modify the excess burst size by toggling the selection in the **Use Default** field to **No**. You can then enter a different excess burst size in the **Value** field.

Note: Some Frame Relay service providers allow for over-subscription of the DLCIs, which occurs when the total number of CIRs for all PVCs exceeds the line rate set up.

5. Select **ADD DLCI NOW** to save the current static Frame Relay DLCI profile that you have just entered, and press Return to go back to the **Frame Relay DLCI Configuration** screen. Alternately, you can cancel the Frame Relay DLCI profile you have just created by selecting **CANCEL** to exit the Add DLCI screen.

Deleting a Frame Relay DLCI configuration

To delete a Frame Relay DLCI configuration, select **Delete DLCI** in the Frame Relay DLCI Configuration screen and press Return to display the Frame Relay DLCI configuration table.

```
                       Frame Relay DLCI Configuration
                      +-DLCI Name----------DLCI Number-+
                      +--------------------------------+
                      | joe                     16 |
     +-----------------------------------------------------------------------+
     +-----------------------------------------------------------------------+
     |                                                                       |
     |  Are you sure you want to delete this DLCI?                           |
     |            CANCEL                         CONTINUE                    |
     |                                                                       |
     +-----------------------------------------------------------------------+
                      |                               |
                      |                               |
                      |                               |
                      |                               |
                      +-------------------------------+
```

1. Highlight the Frame Relay DLCI configuration you wish to delete. Press Return.

2. A Frame Relay DLCI Configuration table appears with a prompt asking you if you want to delete the connection profile you have just highlighted. Select **CONTINUE** if you wish to delete this DLCI or **CANCEL** if you do not.

You are now finished configuring the Frame Relay DLCI Configuration screen.

Part II: Advanced Configuration

Chapter 8

WAN and System Configuration

This chapter describes how to use the console-based management screens to access and configure advanced features of your Netopia R3100 ISDN Router. You can customize these features for your individual setup. These menus provide a powerful method for experienced users to set up their router's connection profiles and system configuration.

This section covers the following topics:

Creating a new Connection Profile

Connection Profiles define the telephone and networking protocols necessary for the router to make a remote connection. A Connection Profile is like an address book entry describing how the router is to get to a remote site, or how to recognize and authenticate a remote user dialing in to the router. For example, to create a new **Connection Profile**, you navigate to the **WAN Configuration** screen from the Main Menu, and select Add Connection Profile.
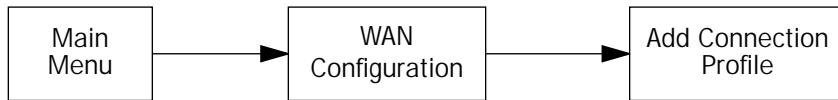
The **Add Connection Profile** screen appears.

```
                         Add Connection Profile
            Profile Name:                    Profile 02
            Profile Enabled:                 Yes

            IP Enabled:                      Yes
            IP Profile Parameters...

            IPX Enabled:                     No


            Data Link Encapsulation...       PPP
            Data Link Options...


            Telco Options...



            ADD PROFILE NOW                  CANCEL

   Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
   Configure a new Conn. Profile. Finished?  ADD or CANCEL to exit.
```

On a Netopia R3100 ISDN Router you can add up to 15 more connection profiles, for a total of 16.

A Netopia R3100 IDSL Router can only use one at a time.

1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.

2. Toggle the **Profile Enabled** value to Yes or No. The default is Yes.

3. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

```
                         IP Profile Parameters


          Address Translation Enabled:      Yes


          Local WAN IP Address:             0.0.0.0

          Remote IP Address:                0.0.0.0
          Remote IP Mask:                   0.0.0.0

          Filter Set...
          Remove Filter Set

          Receive RIP:                      Off




   Toggle to Yes if this is a single IP address ISP account.
   Configure IP requirements for a remote network connection here.
```

4. Toggle or enter any IP Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see "IP Setup and Network Address Translation" on page 11-1.

5. If you will be connecting with an IPX remote network, toggle **IPX Enabled** to Yes, and press Return. Otherwise, accept the default No.

    If you enable IPX routing, an **IPX Profile Parameters** menu item becomes available. Select IPX Profile Parameters and press Return. The IPX Profile Parameters screen appears.

```
                         IPX Profile Parameters

            Remote IPX Network:                     00000000
            Path Delay:                             10
            NetBios Packet Forwarding:              Off

            Incoming Packet Filter Set...           <<NONE>>
            Outgoing Packet Filter Set...           <<NONE>>

            Incoming SAP Filter Set...              <<NONE>>
            Outgoing SAP Filter Set...              <<NONE>>



            Periodic RIP Timer:                     60
            Periodic SAP Timer:                     60




     Configure IPX requirements for a remote network connection here.

```

6. Toggle or enter any IPX Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see "IPX Setup" on page 12-1.

7.   Select **Datalink Options** and press Return. The Datalink Options screen appears.

```
                    Datalink (PPP/MP) Options


        Data Compression...              Ascend LZS

        Send Authentication...           PAP

        Send User Name:
        Send Password:

        Receive User Name:
        Receive Password:

        Channel Usage...                 Dynamic

        Bandwidth Allocation...          BAP

        Maximum Packet Size:             1500



  In this Screen you will configure the PPP/MP specific connection params.
```

You can accept the defaults, or change them if you wish. You can also specify user name and password for both outgoing and incoming calls. the Send User Name/Password parameters are used to specify your identity when dialing out to a remote location. The Receive User Name/Password parameters are used when receiving dial-in clients such as via RAS configuration.

The **Channel Usage** pop-up menu allows you to choose how many lines your connections may use, and whether or not they are preemptable. Supported options are:

Option	Behavior
Dynamic	1 to 3 channels, if available, will be used, depending on traffic volume
1-Channel	Only 1 channel will be used
2-Channels	2 channels will be preferred
2-Channel Preemptable	2 channels will be used, but 1 may be reallocated

Note: The **Bandwidth Allocation** pop-up options are: Off, Auto, BAP or MP+. BAP is the default. You should only choose one of the other options if you are specifically advised to do so by your ISP or administrator.

Return to the Add Connection Profile screen by pressing Escape.

8. Select **Telco Options** and press return. the Telco Options screen appears.

    Note: For IDSL routers, which do not initiate dial-up connections, this option does not appear.

```
                          Telco Options

        Initiate Data Service...          64 kb/sec

        Dial...                           Dial In/Out


        Number to Dial:
        Alternate Site to Dial:

        Dial on Demand:                   Yes
        Idle Timeout (seconds):           300

        CNA Validation Number:
        Callback:                         No

        Maximum connect time (HH:MM):     0:00

 Return/Enter to select data rate/class of service.
 In this Screen you configure options for the ways you will establish a link.
```

Select **Dial** and press Return. A pop-up menu appears. You can select the dialing options for this Connection Profile as Dial In Only, Dial Out Only, or Dial In/Out.

You can:

■   select a type of data service to initiate, 64 kb/sec (the default), 56 kb/sec, or Speech

■   add the number to dial for this Connection Profile

■   add an alternate number

■   change any of the default parameter settings

■   if you have enabled Call Accounting (see "Cost control feature -- call accounting" on page 10-1) you can set the **Maximum connect time** for this connection profile by entering the hours and minutes in HH:MM format. When aggregate usage for this profile reaches this threshold, the profile becomes temporarily disabled until the limit is raised or the counters are reset (see "Viewing call accounting statistics" on page 10-2). If Call Accounting is not enabled, this field does not appear.

When you are finished with these entries, press Escape to return to the **Add Connection Profile** screen.

9. Select **ADD PROFILE NOW** and press Return. Your new Connection Profile will be added.

If you want to view the Connection Profiles in your router, return to the WAN Configuration screen, and select **Display/Change Connection Profile**. The list of Connection Profiles is displayed in a scrolling pop-up screen.
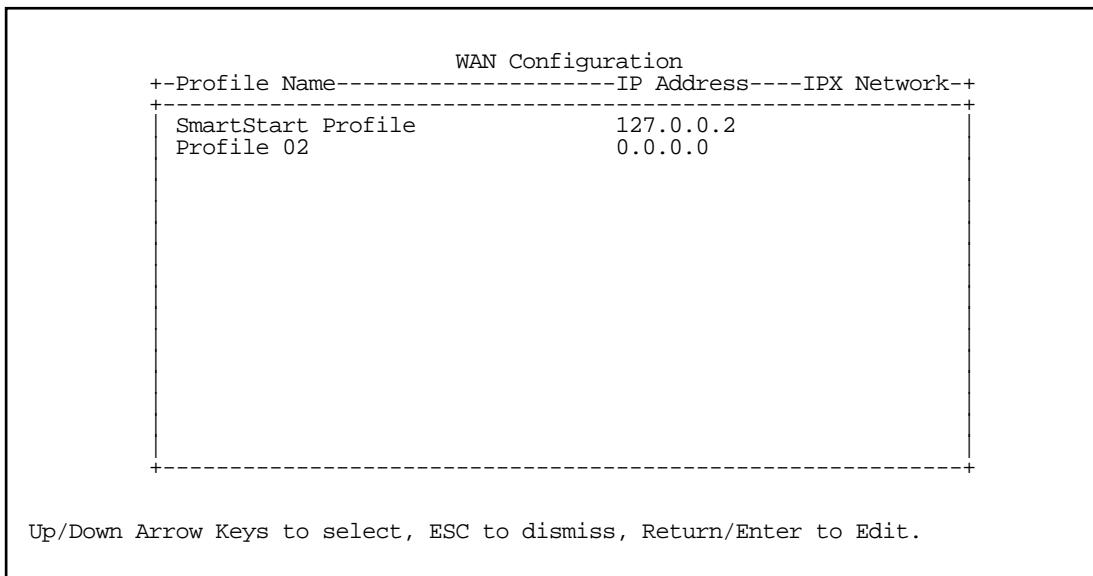
```
                         WAN Configuration
        +-Profile Name-------------------IP Address----IPX Network-+
        +----------------------------------------------------------+
        |  SmartStart Profile                127.0.0.2             |
        |  Profile 02                        0.0.0.0               |
        |                                                          |
        |                                                          |
        |                                                          |
        |                                                          |
        |                                                          |
        |                                                          |
        |                                                          |
        |                                                          |
        |                                                          |
        |                                                          |
        +----------------------------------------------------------+

    Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

It is possible to configure the router for any available circuit type: **ISDN, Switched**, **ISDN, Leased**, **IDSL, Ascend**, or **IDSL, CMN**, depending on the switch gear you are connected to. See the table of configuration options on page 7-4.

If you create a Connection Profile using a particular datalink encapsulation method, that profile will take precedence whenever you connect to a line that uses that datalink encapsulation. If there is no Connection Profile with the datalink encapsulation method that the line uses, the router will default to using the Default Profile. See "The Default Profile," for more information.

The Default Profile

How the default profile works

The default profile works like a guard booth at the gate to your network: it scrutinizes WAN connections. Like the guard booth, the default profile allows connections based on a set of criteria that you define.

The main criterion used to check connections is whether they match one of the connection profiles already defined. A connection is matched to a connection profile using the remote network's IP address (that is, the caller is defined as the destination of a particular connection profile).

If a connection matches an existing profile, all of the connection profile parameters are adopted for the call. When using PPP or Cisco-HDLC datalink encapsulation on a permanent circuit, you must configure a connection profile. Note, that you may have already configured this connection profile in Easy Setup.

See "Easy Setup" on page 7-1 for information on configuring an Easy Setup connection profile.

When using Frame Relay datalink encapsulation on a permanent circuit, you may require that the frame relay DLCIs explicitly match up to your connection profile, or you may allow your Frame Relay network to automatically confirm this by using the Default Profile.

Customizing the Default Profile

The Default Profile screen controls whether or not an IDSL link will come up without an explicitly configured connection profile. See "Creating a new Connection Profile" on page 8-1 for more information. You access the Default Profile screen from the Main Menu by selecting WAN Configuration and then selecting **Default Profile**.

```
┌──────────┐      ┌──────────────┐      ┌──────────┐
│   Main   │─────▶│     WAN      │─────▶│ Default  │
│   Menu   │      │Configuration │      │ Profile  │
└──────────┘      └──────────────┘      └──────────┘
```
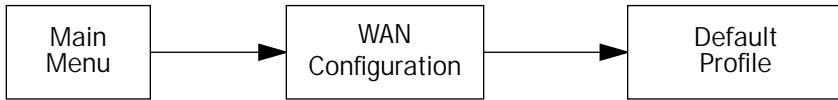
The Default Profile screen appears.

```
                        Default Profile


        Must Match a Defined Profile:        Yes

        IP Enabled:                          Yes
        IP Parameters...

        IPX Enabled:                         Yes
        IPX Parameters...


```

■   You can set **Must Match a Defined Profile** item to **Yes** or **No** (the default). This item controls whether or not the IDSL link will come up without an explicitly configured connection profile. If your ISP is serving you a dynamic IP Address, you need not explicitly configure a connection profile, and the default behavior of the router will be to connect automatically once it is powered on.

■   If Must Match a Defined Profile is set to No, then an **IP Enabled** item is visible. Toggling this item to **Yes** (the default) or **No** controls whether or not IP will be supported on the IDSL link. If IP Enabled is set to Yes, an **IP Parameters** item becomes visible. If you select IP Parameters the IP Parameters screen appears (see "IP parameters (default profile) screen" on page 8-8). This screen allows you to configure various IP parameters for IDSL connections established without an explicitly configured connection profile.

■   If Must Match a Defined Profile is set to No, then an **IPX Enabled** item is visible. Toggling this item to **Yes** or **No** (the default) controls whether or not IPX will be supported on the IDSL link. If IPX Enabled is set to Yes, an **IPX Parameters** item becomes visible. If you select IPX Parameters, the IPX Parameters screen appears (see "IPX parameters (default profile) screen" on page 8-10). This screen allows you to configure various IPX parameters for IDSL connections established without an explicitly configured connection profile.

IP parameters (default profile) screen

The IP Parameters (Default Profile) screen allows you to configure various IP parameters for IDSL connections established without an explicitly configured connection profile:

```
                    IP Parameters (Default Profile)




        Default Subnet Mask:              0.0.0.0

        Filter Set (Firewall)...
        Remove Filter Set

        Receive RIP:                     Both
        Transmit RIP:                    v2 (multicast)
```
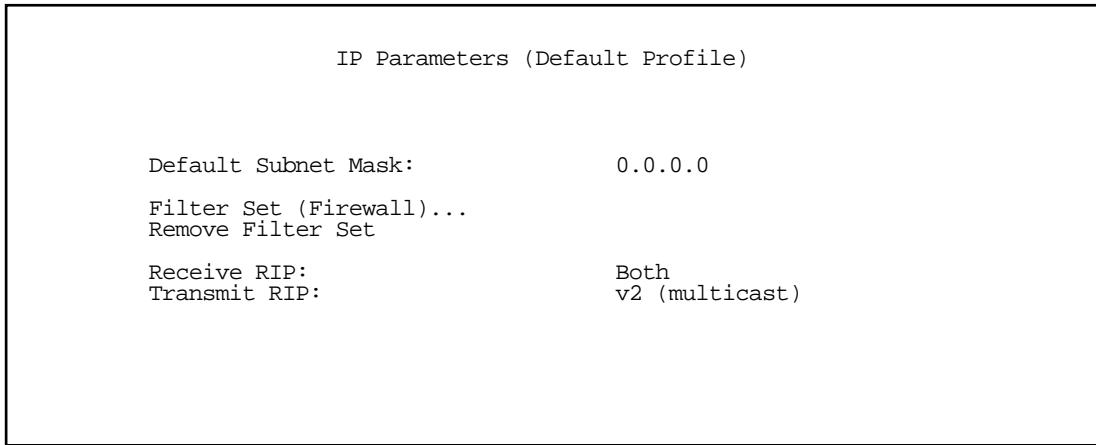
The Netopia R3100 ISDN Router always acts as a DHCP client on the IDSL link when using a Default Profile. The DHCP server will supply a local IP address and subnet mask. For an IDSL link, Network Address Translation (NAT) is enabled by default in the Default Profile and the Default Subnet Mask is set to 0.0.0.0. For details on setting up IP Parameters see "IP Setup and Network Address Translation" on page 11-1.

Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia R3100 needs to recognize. Set to "Both" (the default) the Netopia R3100 will accept information from either RIP v1 or v2 routers. Alternatively, select **Receive RIP** and select **v1** or **v2** from the popup menu. With Receive RIP set to "v1," the Netopia R3100's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to "v2," the Netopia R3100 will accept routing information provided by RIP packets from other routers that use different subnet masks.

If you want the Netopia R3100 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia R3100 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia R3100 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia R3100 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

```
                    IP Parameters (Default Profile)


   Default Subnet Mask:                 0.0.0.0




         Filter Set (Firewall)...
         Remove Filter Set

         Receive RIP:             +------------------+
         Transmit RIP:            +------------------+
         TX RIP Policy...         | Poison Reverse   |
                                  | Split Horizon    |
                                  | No Split Horizon |
                                  +------------------+
```

If you choose to transmit RIP, the TX RIP Policy pop up menu appears. You can select **Poison Reverse** (the default), **Split Horizon**, or **No Split Horizon**.

■ Poison Reverse speeds convergence but adds to network overhead. When topology changes, mentioning routes that should not go through the router as well as those that should can speed up convergence.

■ If you select Split Horizon ("without Poison Reverse" is implied), the router omits routes learned from an interface from RIP updates sent on that interface. Split Horizon without Poison Reverse has the advantage of minimizing network overhead in large network configurations at the expense of slower convergence.

■ No Split Horizon is suitable for partially meshed frame relay networks. A partially meshed network is a WAN in which one or more nodes do not have logically direct connections to all other nodes. In a star or partially meshed Frame Relay topology, you may need to disable Split Horizon so the routers can learn about other networks.

See "Configuring Frame Relay" on page 7-11 and Appendix G, "Understanding Frame Relay," for more information.

IPX parameters (default profile) screen

The IPX Parameters (Default Profile) screen allows you to configure various IPX parameters for IDSL connections established without an explicitly configured connection profile:

```
                    IPX Parameters (Default Profile)

        NetBios Packet Forwarding:          Off
        Path Delay:                         10

        Incoming Packet Filter Set...       <<NONE>>
        Outgoing Packet Filter Set...       <<NONE>>
        Incoming SAP Filter Set...          <<NONE>>
        Outgoing SAP Filter Set...          <<NONE>>


        Periodic RIP Timer:                 60
        Periodic SAP Timer:                 60
```
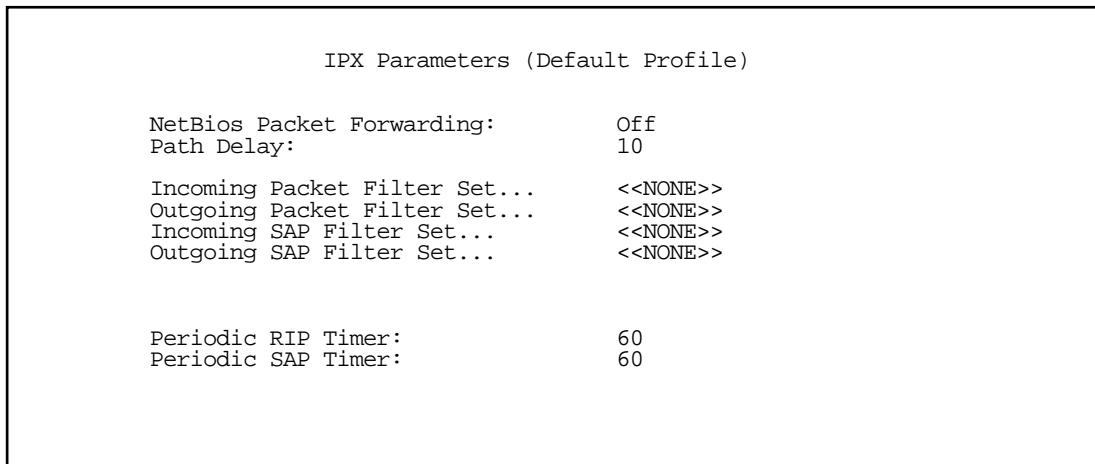
For details on setting up IPX Parameters see "IPX Setup" on page 12-1. For details on setting up Filter Sets see "Security" on page 15-1.

Auxiliary Port Configuration

If your router supports it, the Auxiliary port can be configured through the WAN Configuration screen. IDSL routers do not support this feature. The ISDN Easy Setup screen does not include auxiliary serial port configuration. To configure the auxiliary port for its possible options, from the Main Menu select WAN Configuration and then WAN setup.

```
┌──────────────┐        ┌──────────────┐        ┌──────────────┐
│    Main      │ ──────▶│    WAN       │ ──────▶│    WAN       │
│    Menu      │        │ Configuration│        │   Setup      │
└──────────────┘        └──────────────┘        └──────────────┘
```
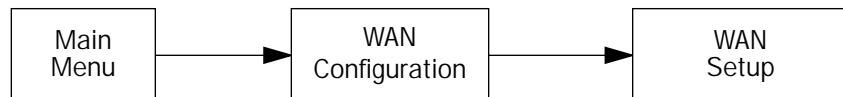
The ISDN Line Configuration screen appears.

```
                        ISDN Line Configuration


          Circuit Type...                   ISDN, Switched
          Switch Type...                    AT&T 5ESS Pt-to-Pt

          Directory Number 1:               555-1234



          PBX Prefix:

          Data Link Encapsulation...        PPP

          Aux Serial Port...                Async Modem
          Data Rate (kbps)...               57.6
          Aux Modem Init String:            AT&F&C1&D2E0S0=1



 Return/Enter to select <among/between> ...
 Enter information supplied to you by your ISDN phone company.
```

By default, the auxiliary port is enabled for an asynchronous modem. You can disable the port by selecting **Unused**, or if you have installed the optional AppleTalk Kit, **LocalTalk** becomes the default. For more information, see Chapter 13, "AppleTalk Setup."

You can specify the **Data Rate** as 19.2, 38.4, 57.6, 115.2, or 230.4. 57.6 is the default.

You can modify the modem init string to conform to your modem's requirements. Refer to your modem's documentation.

Note: When used in conjunction with ISDN, the auxiliary port is only useful for WAN services when the ISDN line is configured for PPP authentication. Also, an ISDN call will not bond with an auxiliary port asynchronous modem call.

System Configuration screens

You can connect to the Netopia R3100's System Configuration screens:

■   Using Telnet with the Router's Ethernet port IP address

■   Through the console port, using a local terminal (see "Connecting a local terminal console cable to your router" on page 6-3)

You can also retrieve the Netopia R3100's configuration information and remotely set its parameters using the Simple Network Management Protocol (see "SNMP" on page 14-12).

Open a Telnet connection to the IP address you set in the router with SmartStart, for example "192.168.1.1."

The console screen will open to the **Main Menu**, similar to the screen shown below:

```
                          Netopia R3100-UP v4.3


                    Easy Setup...

                    WAN Configuration...

                    System Configuration...

                    Utilities & Diagnostics...

                    Statistics & Logs...

                    Quick Menus...

                    Quick View...
       Return/Enter goes to Easy Setup -- minimal configuration.
       You always start from this main screen.
```
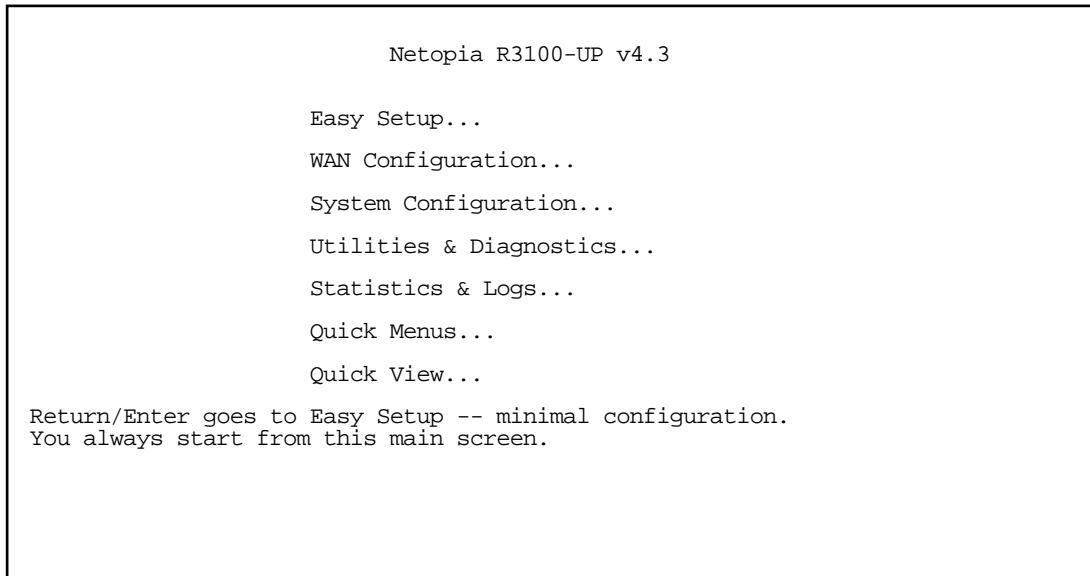
System Configuration *features*

SmartStart may be all you need to configure your Netopia R3100. Some users, however, require advanced settings or prefer manual control over the default selections that SmartStart automatically chooses. For these users, the Netopia R3100 provides System Configuration options.

To help you determine whether you need to use the System Configuration options, review the following requirements. If you have one or more of these needs, use the System Configuration options described in the later chapters.

- Two or more outgoing connection profiles to connect to more than one remote location (for example, to connect to the Internet and to a network at another office).

- System Configuration of dynamic IP address distribution through DHCP, MacIP, or BootP.

- Customized incoming call profile to control received calls.

- Scheduled connections.

- Greater network security through the use of filters, CallerID, callback, and SecurID.

- System Configuration of AppleTalk LAN settings.

- System Configuration of connections to AppleTalk networks through the Internet or any IP network, using AURP (AppleTalk "tunneling").

- System Configuration of connection profiles. See the table below for a partial list of the options available

through System Configuration.

Layer Category	Parameter Type	Options	Default settings
Protocol Layer	IP Parameters	Filter Sets:	Basic Firewall
		RIP Receive/Transmit options:	Off
	IPX Parameters	Path Delay:	1 second
		NetBios Packet Forwarding:	Off
		Incoming/outgoing Packet & SAP filter:	Off
		Periodic RIP/SAP timers:	60 seconds
Datalink Layer	PPP/MP Parameters	Data Compression:	Ascend LZS
		Send Authentication:	PAP
		Channel Usage:	Dynamic
		Bandwidth Allocation:	BAP
		Maximum Packet Size:	1500
Physical Layer	Telco Parameters	Dial is set to:	Dial In/Out
		Dial On Demand is set to:	Yes
		Callback is set to:	No
		Idle Time-out is set for:	300 seconds

To access the System Configuration screens, select **System Configuration** in the Main Menu, then press Return.

The System Configuration screen appears:

```
                        System Configuration


              Network Protocols Setup...
              Filter Sets (Firewalls)...
              IP Address Serving...

              Date and Time...

              Console Configuration...

              SNMP (Simple Network Management Protocol)...

              Security...

              Upgrade Feature Set...

              Telephone Setup...

              Logging...

  Return/Enter to configure Networking Protocols (such as TCP/IP).
  Use this screen if you want options beyond Easy Setup.
```
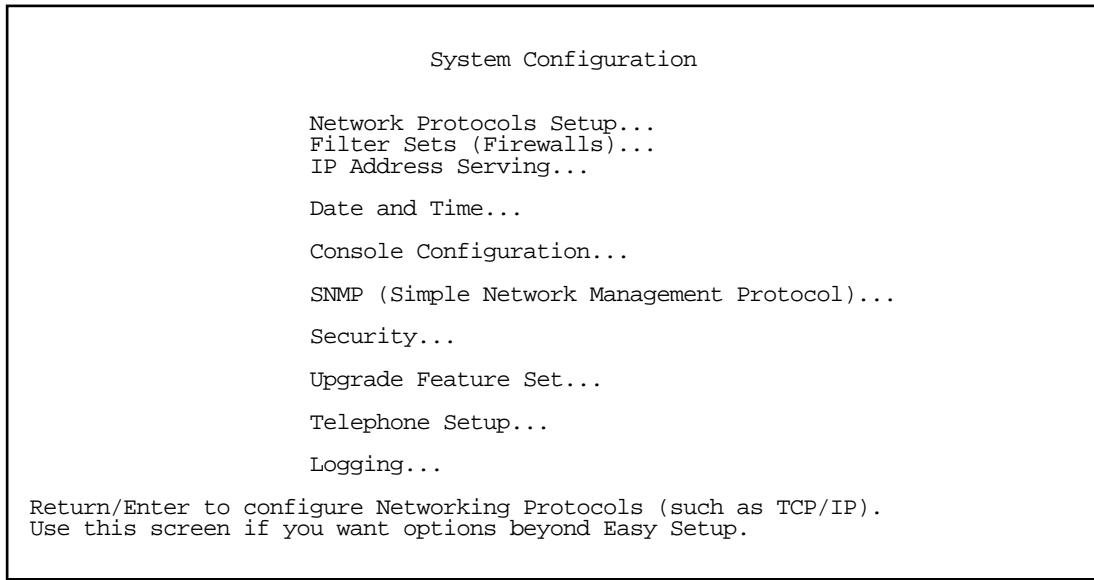
Network Protocols Setup

These screens allow you to configure your network's use of the standard networking protocols:

- IP: details are given in "IP Setup and Network Address Translation" on page 11-1.

- IPX: details are given in "IPX Setup" on page 12-1.

- AppleTalk: details are given in "AppleTalk Setup" on page 13-1.

   Note: AppleTalk requires the optional AppleTalk feature expansion kit.

Filter Sets (Firewalls)

These screens allow you to configure security on your network by means of filter sets and a basic firewall.

- Details are given in "Security" on page 15-1.

IP Address Serving

These screens allow you to configure IP Address serving on your network by means of DHCP, WANIP, BootP, and with the optional AppleTalk kit, MacIP.

- Details are given in "IP address serving" on page 11-16.

Date and Time

You can set the system's date and time in the **Set Date and Time** screen.

Select **Date and Time** in the System Configuration screen and press Return to go to the Set Date and Time screen.

```
                              Set Date and Time


        System Date Format:                      MM/DD/YY
        Current Date (MM/DD/YY):                 3/16/1998

        System Time Format:                      AM/PM
        Current Time:                            10:29
        AM or PM:                                AM
```

Follow these steps to set the system's date and time:

1. Select **Current Date** and enter the date in the appropriate format. Use one- or two-digit numbers for the month and day, and the last two digits of the current year. The date's numbers must be separated by forward slashes (/).

2. Select **Current Time** and enter the time in the format HH:MM, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.

3. Select **AM or PM** and choose **AM** or **PM**.

Console Configuration

You can change the default terminal communications parameters to suit your requirements.

To go to the Console Configuration screen, select **Console Configuration** in the System Configuration screen.

```
                        Console Configuration


        Baud Rate...                            9600

        Hardware Flow Control:                  No






        SET CONFIG NOW                          CANCEL



```
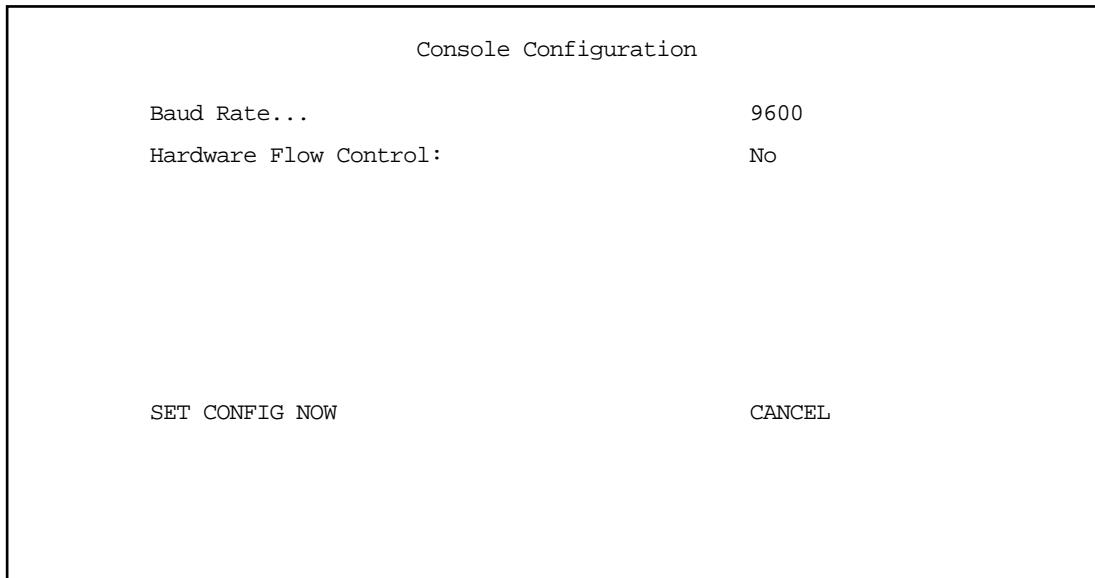
Follow these steps to change a parameter's value:

1. Select the parameter you want to change.

2. Select a new value for the parameter. Return to step 1 if you want to configure another parameter.

3. Select **SET CONFIG NOW** to save the new parameter settings. Select **CANCEL** to leave the parameters unchanged and exit the Console Configuration screen.

SNMP (Simple Network Management Protocol)

These screens allow you to monitor and configure your network by means of a standard Simple Network Management Protocol (SNMP) agent.

■   Details are given in "SNMP" on page 14-12.

Security

These screens allow you to add users and define passwords on your network.

■   Details are given in "Security" on page 15-1.

Upgrade Feature Set

You can upgrade your Netopia R3100 by adding new feature sets through the **Upgrade Feature Set** utility.

See the release notes that came with your router or feature set upgrade or visit the Netopia web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Netopia R3100.

Telephone setup

With SmartPhone, analog devices such as telephones, facsimile machines, or modems can connect to the Netopia Router and communicate over the ISDN line. The Netopia Router with SmartPhone provides:

■   full call routing between directory numbers and phone jacks

■   inbound and outbound call preemption

■   priority ringing based on CallerID

Note: To see whether your Netopia Router supports SmartPhone, look for the two RJ-11 jacks, marked Phone 1 and Phone 2, on the back of the router.

If your router supports the SmartPhone feature refer to "Using SmartPhone for Telephone Services" on page 9-1. If your Netopia R3100 does not support SmartPhone, you can skip this chapter.

Logging

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the router's WAN Event History. See "WAN Event History" on page 14-6.

Select **Logging** from the System Configuration menu.

The Logging Configuration screen appears.

```
                        Logging Configuration


            WAN Event Log Options
            Log Boot and Errors:                 Yes
            Log Line Specific:                   Yes
            Log Connections:                     Yes
            Log PPP, DHCP, CNA:                  Yes
            Log IP and IPX:                      Yes

            Syslog Parameters
            Syslog Enabled:                      No
            Hostname or IP Address:
            Facility...                          Local 0






    Return/Enter accepts * Tab toggles * ESC cancels.

```

By default, all events are logged in the event history.

■   By toggling each event descriptor either **Yes** or **No**, you can determine which ones are logged and which are

ignored.

■   You can enable or disable the syslog client dynamically. When enabled, it will report any appropriate and previously unreported events.

■   You can specify the syslog server's address either in dotted decimal format or as a DNS name up to 63 characters.

■   You can specify the UNIX syslog Facility to use by selecting the **Facility** pop-up.

The following screen shows a sample syslog dump of WAN events:

```
Nov  5 10:14:06 tsnext.farallon.com   Link 1 down: PPP PAP failure
Nov  5 10:14:06 tsnext.farallon.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.farallon.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.farallon.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.farallon.com   Link 1 down: Manual disconnect
Nov  5 10:14:06 tsnext.farallon.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.farallon.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.farallon.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.farallon.com   Link 1 down: No answer
Nov              5          10:14:06          tsnext.farallon.com          --Device
restarted----------------------------------------
Nov  5 10:14:06 tsnext.farallon.com >>Received Speech Setup Ind. from DN: (not supplied)
Nov  5 10:14:06 tsnext.farallon.com   Requested Connect to our DN: 5108645534
Nov  5 10:14:06 tsnext.farallon.com   ASYNC: Modem carrier detected (more) Modem reports: 26400
V34
Nov  5 10:14:06 tsnext.farallon.com >>WAN: 56K Modem 1 activated at 115 Kbps
Nov  5 10:14:06 tsnext.farallon.com   Connect Confirmed to our DN: 5108645534
Nov  5 10:14:06 tsnext.farallon.com   PPP: Channel 1 up, Answer Profile name: Default Profile
Nov  5 10:14:06 tsnext.farallon.com   PPP: NCP up, session 1, Channel 1 Final (fallback)
negotiated auth: Local PAP , Remote NONE
Nov  5 10:14:06 tsnext.farallon.com   PPP: PAP  we accepted remote, Channel 1 Remote name: guest
Nov  5 10:14:06 tsnext.farallon.com     PPP: MP negotiated, session 1 Remote EDO: 06 03
0000C5700624 0
Nov  5 10:14:06 tsnext.farallon.com    PPP: CCP negotiated, session 1, type: Ascend LZS Local
mode: 1, Remote mode: 1
Nov  5 10:14:06 tsnext.farallon.com  PPP: BACP negotiated, session 1 Local MN: FFFFFFFF, Remote
MN: 00000001
Nov  5 10:14:06 tsnext.farallon.com    PPP: IPCP negotiated, session 1, rem: 192.168.10.100
local: 192.168.1.1
Nov  5 10:14:06 tsnext.farallon.com >>WAN: 56K Modem 1 deactivated
Nov  5 10:14:06 tsnext.farallon.com   Received Clear Ind. from DN: 5108645534, Cause: 0
Nov  5 10:14:06 tsnext.farallon.com   Issued Clear Response to DN: 5108645534
Nov  5 10:14:06 tsnext.farallon.com   Link 1 down: Remote clearing
Nov  5 10:14:06 tsnext.farallon.com   PPP: IPCP down, session 1
Nov  5 10:14:06 tsnext.farallon.com >>Received Speech Setup Ind. from DN: (not supplied)
```

Chapter 9

Using SmartPhone for Telephone Services

This chapter describes how to use the Netopia R3100's SmartPhone™ feature. To see whether your Netopia Router supports SmartPhone, look for the two RJ-11 jacks, marked Phone 1 and Phone 2, on the back of the router. If your Netopia R3100 does not support SmartPhone, you can skip this chapter. With SmartPhone, other analog devices such as telephones, facsimile machines, or modems can connect to the Netopia R3100 and communicate over the same lines. The Netopia R3100 with SmartPhone provides:

■   auxiliary telephone control, allowing management of whether an attached phone can pre-empt or interfere with a Netopia R3100 data call. This is also called Call Bumping.

■   off-hook detection, preventing the Netopia R3100 from initiating data calls when the ISDN line is busy with a voice call

■   distinctive ring patterns to identify incoming caller

■   Bellcore specification Caller ID support for call authentication

■   call hold, call retrieve and the Flexible Call Offering (FCO) features known as Conference, Drop, and Transfer

   Note: Outside North America your telephone provider may not use Bellcore specification equipment, thus disabling this feature. Caller ID is received as universally recognizable D channel traffic. The Netopia R3100 generates Bellcore Caller ID to the POTS jacks, which may not be the same encoding as non-North American PTTs use. Therefore an external caller ID box may not work. The Netopia R3100 generates the distinctive ring from the inbound caller ID.

Topics in this chapter include:

■   "Specifying telephone connections" on page 9-1

■   "Defining priority ringing" on page 9-4

■   "Advanced calling features" on page 9-5

Specifying telephone connections

You can configure telephone connections in the Telephone Connections screen, located in the System Configuration screen under **Telephone Setup**.

```
┌──────────┐        ┌──────────────┐        ┌──────────┐
│   Main   │───────▶│    System    │───────▶│ Telephone│
│   Menu   │        │Configuration │        │   Setup  │
└──────────┘        └──────────────┘        └──────────┘
```
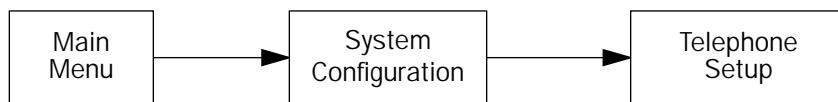
From the System Configuration screen select **Telephone Setup**. The Telephone setup screen appears.

```
                          Telephone Setup


                Telephone Connection...
                Priority Ringing...
                Supplementary Services...













    Return/Enter to configure telephone connections.
    From here you will configure telephone information.
```
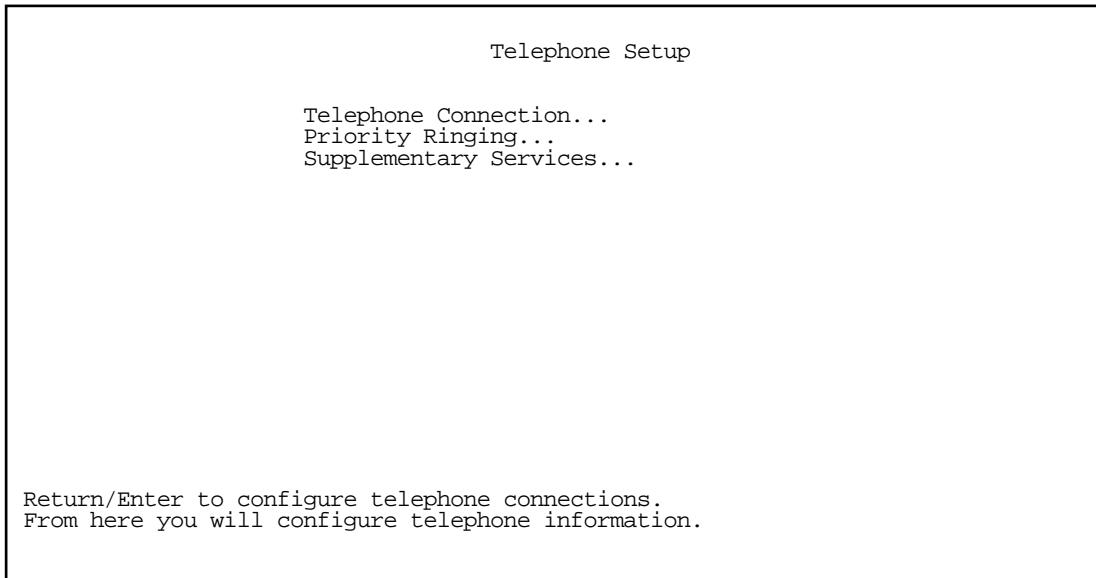
Select **Telephone Connections**. The Telephone connections screen appears.

```
                       Telephone Connections
            Inbound:
                 Directory Number 1 Connection:    Phone 1
                 Directory Number 2 Connection:    Phone 2

            Outbound:
                 Phone 1 Connection:               Either
                 Phone 1 Service Grade:            Speech

                 Phone 2 Connection:               Either
                 Phone 2 Service Grade:            Speech







    Return/Enter for connection list.
    Connect incoming calls and outgoing calls.
```
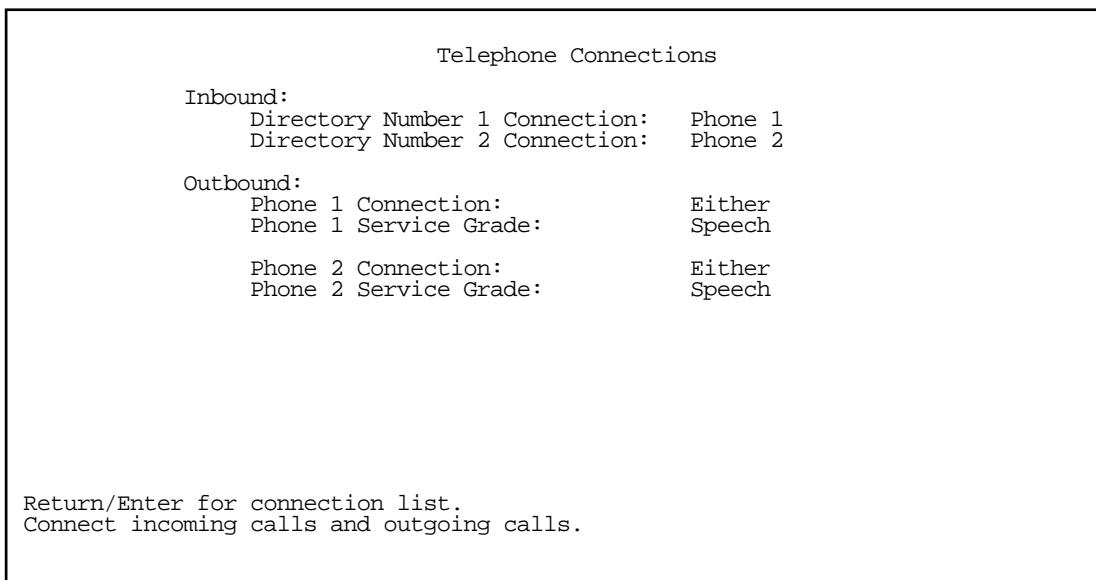
The Telephone Connections screen is divided into two categories, Inbound and Outbound.

■   Inbound determines how an incoming speech call is directed through the Netopia R3100. An incoming call can enter via either of two directory numbers, and can be routed to the phone jacks, used internally by the Router, or blocked.

■   Outbound controls the way a call from a given phone jack is sent from the Netopia Router. It directs which

directory number to use and what kind of transmission service to use.

To configure telephone connections:

1. For **Inbound Directory Number 1 Connection**, press Return and choose one of the following selections from the pop-up menu:

   ■   **Reject as Busy** blocks calls, issuing a busy tone to the party trying to dial in.

   ■   **Phone 1** directs calls out the Netopia Router's Phone 1 jack, ringing the phone or device plugged into that jack.

   ■   **Phone 2** directs calls out the Netopia Router's Phone 2 jack, ringing the phone or device plugged into that jack.

   ■   **Phone 1 & Phone 2** rings all devices connected to the Phone 1 and Phone 2 jacks.

   ■   **Router** directs the incoming call, usually a data-over-voice call with a speech or 3.1 kHz service, internally for the Router's use.

2. For **Inbound Directory Number 2 Connection**, press Return and configure as described in step 1. If no number is entered for Directory Number 2 in the initial configuration, the option you select is stored but not used.

3. For **Outbound Phone 1 Connection**, press Return and choose one of the following selections from the pop-up menu:

   ■   **Blocked** prevents outbound calls on that jack. Devices on that line hear a busy signal. Inbound calls are still possible, depending on how the Netopia Router is configured in steps 1 and 2.

   ■   **Directory Number 1** routes the outbound call out the number specified by Directory Number 1. This ensures that the call is made from the directory number you choose.

   ■   **Directory Number 2** routes outbound calls out the number specified by Directory Number 2.

   ■   **Either** routes outbound calls out either Directory Number 1 or Directory Number 2, depending on which is available, if either.

4. For **Outbound Phone 1 Service Grade**, press Return and choose one of the following selections from the pop-up menu:

   ■   **Speech** for typical speech grade service used in telephone conversations.

   ■   **3.1 kHz Audio** for a higher grade of service that ensures better line conditions for data transfer such as for a facsimile machine or modem.

   Note: The 3.1 kHz service may not be available from your ISDN service provider, and there may be higher tariffs for its use. Check with your ISDN service provider about the availability of this service grade.

5. For **Outbound Phone 2 Connection**, press Return and configure as described in step 3.

6. For **Outbound Phone 2 Service Grade**, press Return and configure as described in step 4.

Defining priority ringing

Priority ringing allows a distinctive ring to be attached to up to 10 incoming caller identifications. For example, a United Kingdom-style ringing pattern can be used to identify calls originating from your home number.

You set priority ringing in the Priority Ringing screen. From the Main Menu go to System Configuration and then Telephone Setup. Select **Priority Ringing** and press Return. The Priority Ringing screen appears.

```
                         Priority Ringing

                  Caller ID              Ringing Tone
            1: 201-555-9911                 Normal
            2: 415-321-6223                 Double Ring
            3: 508-896-2310                 Silence
            4: 510-545-6645                 PBX
            5: 408-533-7890                 Distinctive 2
            6: 212-491-3698                 Distinctive 1
            7:                              Normal
            8:                              Normal
            9:                              Normal
           10:                              Normal

                         PREVIEW RING




  Enter Caller ID
  You can enter a list of Caller IDs and associate a ringing tone with each ID.
```
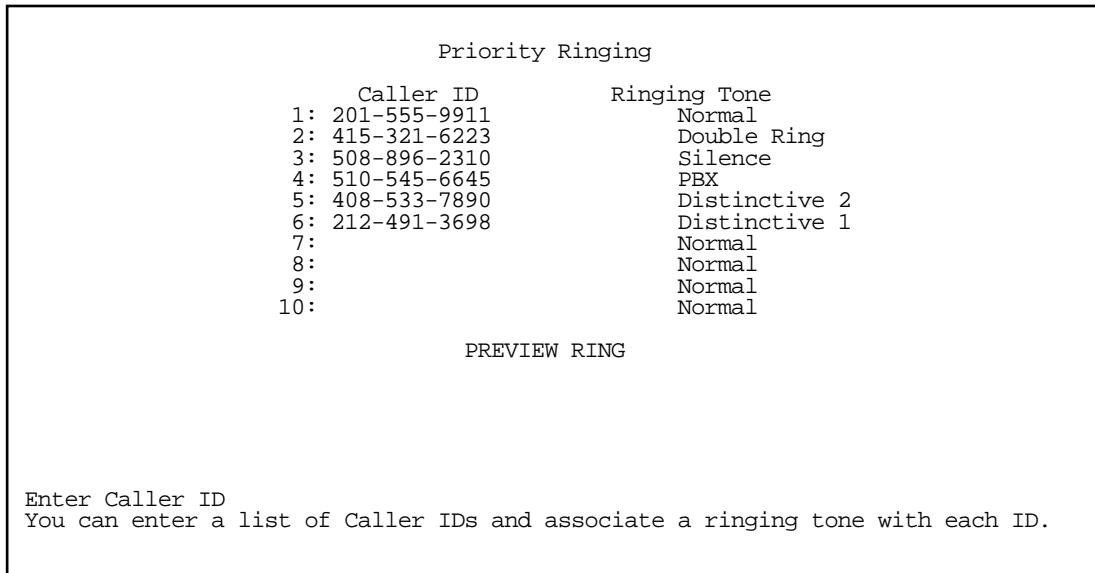
To set up priority ringing:

1. For CallerID, enter a telephone number sequence. Observe the following guidelines:

    ■ The following characters are acceptable:
    0 1 2 3 4 5 6 7 8 9 . ( ) / - ?

    Other characters are invalid and cause the entire entry to be rejected.

    ■ The **?** character represents a single-digit wildcard. While matching the incoming caller identification with the priority ringing CallerIDs, any digit is considered to be a match at the location where the **?** appears. For example, the caller identification **415-555-111?** matches incoming numbers **415-555-1112** and **415-555-1113** for priority ringing.

    ■ The maximum entry length is 20 characters. Longer entries are rejected. Note, however, that telephone numbers consist of a maximum of 10 digits. For internal matching against an incoming call, the Netopia Router removes all characters that are not digits or wildcards.

2. For **Ringing Tone**, press Return and select one of the ringing patterns listed in the pop-up menu.

3. To test a ringing pattern, highlight **Preview Ring** and press Return. Select one of the ringing patterns listed in the pop-up menu. When one or more telephones are hooked up to either of the Phone 1 or Phone 2 jacks, the pattern rings briefly on the telephones not in use.

Advanced calling features

The Netopia R3100 ISDN Router supports call hold, call retrieve and the Flexible Call Offering (FCO) features known as Conference, Drop, and Transfer. This allows multiple services to be performed using only the hook-switch as an activator.

Note: A flash hook is currently defined as one on hook/off hook transition of at least 200 ms, but not greater than 1.3 seconds. A double flash hook is currently defined as two on hook/off hook transitions of at least 200 ms, with both completing in 1.3 seconds.

■   While a call is active, you can initiate a single flash hook to start a second call. This will place the first call on hold, and provide a dial tone. Two individual active calls per channel are allowed.

■   Once the second call is established, you can switch back and forth between the two calls by sending a single flash hook.

■   If you want to conference two calls that are active (one on hold, and one live) send a double flash hook to activate the conference, followed by a single flash hook to bridge the calls together. This process can be repeated to bridge additional users to the conference, up to the maximum allowed by the line's provisioning.

■   If a conference is active, you can drop the last call added to the conference by issuing a double flash hook.

■   If you want to transfer an active conference (allow the two calls to continue to talk after the Netopia R3100 has disconnected), send a single flash hook to receive a new dial tone, followed by a double flash hook to initiate the transfer.

Line provisioning

NI-1 and DMS-100 custom lines use the Q.932 protocol (an extension to Q.931) for hold/retrieve and Flexible Calling services. For Conference, Drop, and Transfer, the services are initiated via a "key ID" informational message. The Netopia R3100's Key settings and the ISDN line's provisioning must match for a feature to work. The Netopia R3100 currently uses a default of 7,8,9 for Conference, Drop, and Transfer, respectively. Defaults vary by switch manufacturer. Some common examples are:

■   BellCore: 60, 61, 62

■   Ascend (old): 6, 7, 8

■   PacBell: 7, 8, 9 and 17, 18, 19

The range is 1 through 64, with many phone companies using 1 through 9 to save memory.

Configuring supplementary services

You set up supplementary services in the Supplementary Services screen. From the Main Menu go to System Configuration and then Telephone Setup. Select **Supplementary Services** and press Return. The Supplementary Services screen appears.

```
                         Supplementary Services


             Flash Hook Enabled:              Yes
             Double Flash Hook Enabled:       Yes

             Conference ID (1..64):           7
             Drop ID (1..64):                 8
             Transfer ID (1..64):             9








     Allow Flash Hook to perform hold and retrieve held POTS calls.
     Setup Hold, Drop, Transfer, and Conference features.
```

Both Flash Hook and Double Flash Hook are enabled by default. You can toggle either or both to **Yes** or **No**.

For the three key ID settings, consult your telephone company, and either request that they provision your line to the Netopia R3100's defaults, or change the defaults to match your telephone company's provisioning.

Chapter 10

Call Accounting and Default Answer Profile

You can set a Netopia Router to make scheduled connections using designated connection profiles. This is useful for creating and controlling regularly scheduled periods when the router can be used by hosts on your network. It is also useful for once-only connections that you want to schedule in advance. For IDSL routers, which do not make dial-up connections, these options does not appear and you can skip this chapter.

The Netopia R3100 ISDN Router can also answer calls as well as initiate them. To answer calls, the Netopia R3100 uses a Default Answer Profile. The Default Answer Profile controls how incoming calls are set up, authenticated, filtered, and more.

Topics in this chapter include:

- ■ "Cost control feature -- call accounting" on page 10-1
- ■ "Scheduled connections" on page 10-4
- ■ "Default Answer Profile" on page 10-9

Cost control feature -- call accounting

The Netopia R3100 offers system-wide and per connection profile call accounting to track first minutes (an ISDN tariff factor) and additional minutes, for initiated data and voice calls.

```
┌───────────┐      ┌─────────────────┐      ┌──────────────────┐
│   Main    │ ───▶ │      WAN        │ ───▶ │  Call Accounting │
│   Menu    │      │  Configuration  │      │   Configuration  │
└───────────┘      └─────────────────┘      └──────────────────┘
```

To go to the Call Accounting screen, select **Call Accounting Configuration** in the WAN Configuration screen.

```
                    Call Accounting Configuration

    Enable Call Accounting:          On

    Day for auto-reset of timers:    12

    Maximum Aggregate connect time:  12:00
```

To enable call accounting, follow these steps:

1. Select **Enable Call Accounting** and toggle it to **On**.

2. Select **Day for auto-reset of timers** and enter the day of the month for the Router to reset the Call Account-ing Statistics.

3. Select **Maximum Aggregate connect time (HH:MM)** and enter the total amount of time to allow for out-bound calls, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.

Viewing call accounting statistics

To view call accounting statistics, go to the Statistics & Logs screen from the Main Menu and select **Call Accounting Statistics**.

```
  ┌──────────┐      ┌──────────────┐      ┌──────────────────┐
  │  Main    │ ───▶ │ Statistics & │ ───▶ │ Call Accounting  │
  │  Menu    │      │    Logs      │      │   Statistics     │
  └──────────┘      └──────────────┘      └──────────────────┘
```

The Call Accounting Statistics screen appears.

```
                        Call Accounting Statistics


                    Aggregate Statistics...

                    Profile Statistics...
```
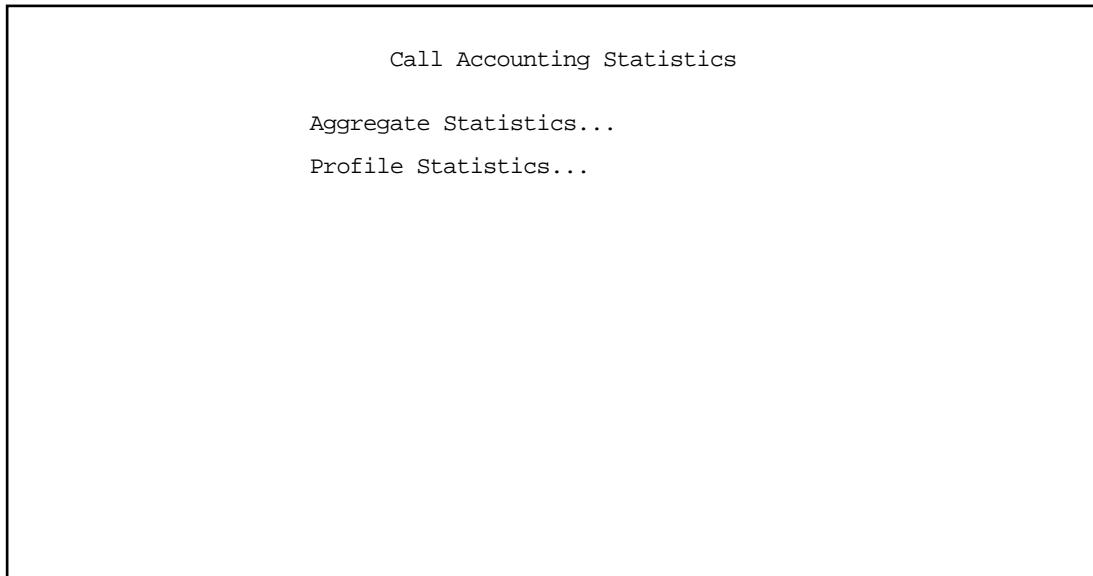
If you select **Aggregate Statistics**, the following screen appears.

```
                    Call Accounting Aggregate Statistics


        Total First Minutes:                0
        Total Additional Time (HH:MM):      0:00

        Remaining Time (HH:MM):             12:00

                        RESET AGGREGATE MINUTE COUNTERS










    Hit Return or Enter to reset Total First/Additional Time.
```
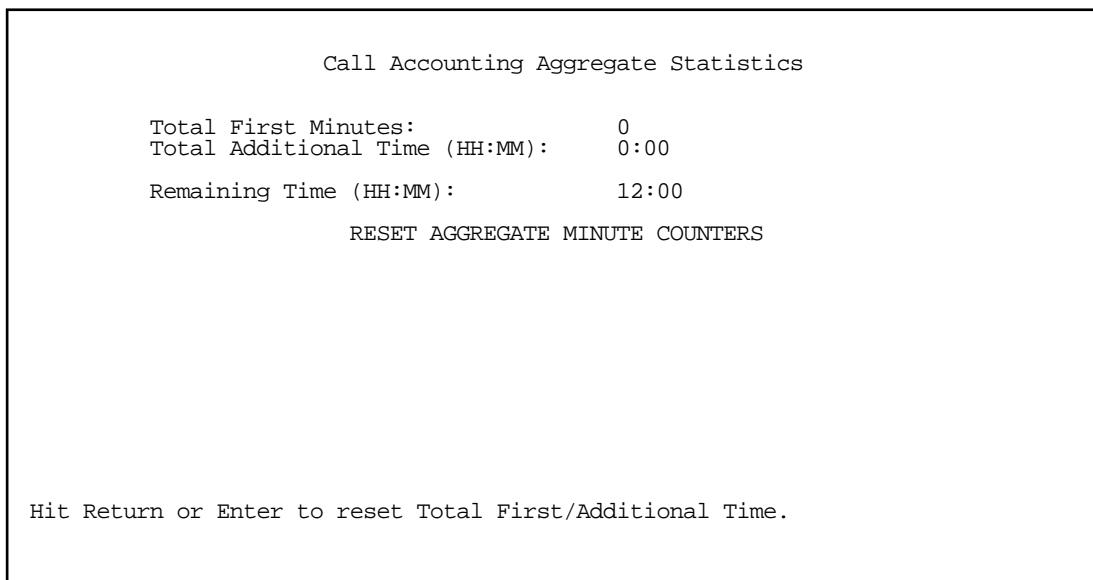
■ **Total First Minutes** displays the total number of first minutes of outbound calls placed during the recording interval.

■ **Total Additional Minutes (HH:MM)** displays the total remaining time of all outbound calls placed during the recording interval.

■ **Remaining Time (HH:MM)** displays how much time is left in the recording interval. If call accounting is not

enabled, the message will read, Call Accounting Disabled.

■   You can reset the counters by selecting **RESET AGGREGATE MINUTE COUNTERS**. A dialog box will ask you to confirm the reset. Select **CONTINUE** to reset the counters or **CANCEL** to leave them as is.

If you select **Profile Statistics**, the following screen appears.

```
            Call Accounting Profile Statistics (in HHHH:MM)

Profile Name---------First Minutes----Additional Minutes-------Cutoff--Expired
-------------------------------SCROLL UP----------------------------------
Easy Setup Profile               0:00                    0:00           0:00




                        




                        -------------------------------SCROLL DOWN-------------------------------

```

You can view the individual usage statistics for each of the Connection Profiles you have defined.

Scheduled connections

To go to the Scheduled Connections screen, select **Scheduled Connections** in the WAN Configuration screen.
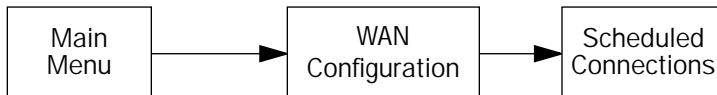
```
                         Scheduled Connections

                  Display/Change Scheduled Connection...

                  Add Scheduled Connection...

                  Delete Scheduled Connection...




    Navigate from here to add/modify/change/delete Scheduled Connections.
```

Viewing scheduled connections

To display a table of view-only scheduled connections, select **Display/Change Scheduled Connection** in the Scheduled Connections screen. Each scheduled connection occupies one row of the table.

```
                         Scheduled Connections

    +-Days----Begin At---HH:MM---When----Conn. Prof. Name----Enabled-----+
    +--------------------------------------------------------------------+
    |  mtWtfss 08:30PM    06:00    weekly   Profile 01          No        |
    |                                                                     |
    |                                                                     |
    |                                                                     |
    |                                                                     |
    +--------------------------------------------------------------------+
```

The first column in the table shows a one-letter representation of the **Days** of the week, from Monday (M or m) to Sunday (S or s). If a letter representing a day is capitalized, the connection will be activated on that day; a lower-case letter means that the connection will not be activated on that day. If the scheduled connection is configured for a once-only connection, the word "once" will appear instead of the days of the week.

The other columns show:

■ The time of day that the connection will **Begin At**

■ The duration of the connection (**HH:MM**)

■ Whether it's a recurring **Weekly** connection or used **Once Only**

■ Which connection profile (**Conn. Prof.**) is used to connect

■ Whether the scheduled connection is currently **Enabled**

The router checks the date and time set in scheduled connections against the system date and time.

Adding a scheduled connection

To add a new scheduled connection, select **Add Scheduled Connection** in the Scheduled Connections screen and press Return. The Add Scheduled Connection screen appears.

```
                    Add Scheduled Connection

       Scheduled Connection Enable:            On

       How Often...                            Weekly

       Schedule Type...                        Forced

       Set Weekly Schedule...

       Use Connection Profile...




          ADD SCHEDULED CONNECTION                  CANCEL

     Scheduled Connections dial remote Networks on a Weekly or Once-Only basis.
```
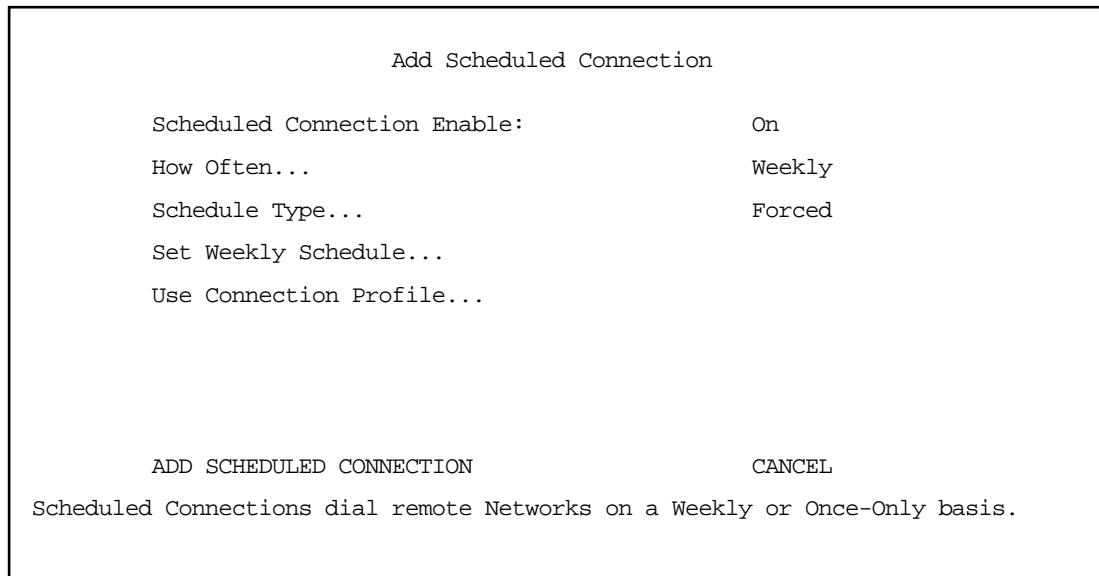
Follow these steps to configure the new scheduled connection:

■ To activate the connection, select **Scheduled Connection Enable** and toggle it to **On**. You can make the scheduled connection inactive by toggling **Scheduled Connection Enable** to **Off**.

■ Decide how often the connection should take place by selecting **How Often** and choosing **Weekly** or **Once Only** from the pop-up menu.

■ The **Schedule Type** allows you to set the exact weekly schedule or once-only schedule.

Options are:

  ■ **Forced Up**, meaning that this connection will be maintained whether or not there is a demand call on the line.

  ■ **Forced Down**, meaning that this connection will be torn down or blocked whether or not there is a

demand call on the line.

- ■ **Demand-Allowed**, meaning that this schedule will permit a demand call on the line.

- ■ **Demand-Blocked**, meaning that this schedule will prevent a demand call on the line.

- ■ **Periodic**, meaning that the connection is retried several times during the scheduled time.

- ■ If **How Often** is set to **Weekly**, the item directly below **How Often** reads **Set Weekly Schedule**. If **How Often** is set to **Once Only**, the item directly below **How Often** reads **Set Once-Only Schedule**.

Set Weekly Schedule

If you set **How Often** to **Weekly**, select **Set Weekly Schedule** and go to the Set Weekly Schedule screen.

- ■ Select the days for the scheduled connection to occur and toggle them to **Yes**.

```
                          Set Weekly Schedule


          Monday:                               No
          Tuesday:                              No
          Wednesday:                            No
          Thursday:                             No
          Friday:                               No
          Saturday:                             No
          Sunday:                               No

          Scheduled Window Start Time:          11:50
          AM or PM:                             AM

          Scheduled Window Duration Per Day:    00:00
```

- ■ Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.

- ■ You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.

- ■ Select **AM or PM** and choose **AM** or **PM** from the pop-up menu.

- ■ Select **Scheduled Window Duration Per Day** and enter the maximum duration allowed for this scheduled connection, per call.

  You are finished configuring the weekly options. Return to the Add Scheduled Connection screen to continue.

Set Once-Only Schedule

If you set **How Often** to **Once Only**, select **Set Once-Only Schedule** and go to the Set Once-Only Schedule screen.

```
                         Set Once-Only Schedule

      Place Call on (MM/DD/YY):              05/07/1998

      Scheduled Window Start Time:           11:50
      AM or PM:                              AM

      Scheduled Window Duration:             00:00
```

■   Select **Place Call On (Date)** and enter a date in the format MM/DD/YY or MM/DD/YYYY (month, day, year).

   Note: You must enter the date in the format specified. The slashes are mandatory. For example, the entry 5/7/98 would be accepted as May 7, 1998. The entry 5/7 would be rejected.

■   Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.

   Note: You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.

■   Select **AM or PM** and choose **AM** or **PM**.

■   Select **Scheduled Window Duration** and enter the maximum duration allowed for this scheduled connection. Use the same format restrictions noted above.

You are finished configuring the once-only options. Return to the Add Scheduled Connection screen to continue.

■   In the Add Scheduled Connection screen, select **Use Connection Profile** and choose from the list of connection profiles you have already created. A scheduled connection must be associated with a connection profile to be useful. The connection profile becomes active during the times specified in the associated scheduled connection, if any exists.

■   Select **ADD SCHEDULED CONNECTION** to save the current scheduled connection. Select **CANCEL** to exit

the Add Scheduled Connection screen without saving the new scheduled connection.

Modifying a scheduled connection

To modify a scheduled connection, select **Change Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and go to the Change Scheduled Connection screen. The parameters in this screen are the same as the ones in the Add Scheduled Connection screen (except that **ADD SCHEDULED CONNECTION** and **CANCEL** do not appear). To find out how to set them, see "Adding a scheduled connection" on page 10-6.

Deleting a scheduled connection

To delete a scheduled connection, select **Delete Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and press the Return key to delete it. To exit the table without deleting the selected scheduled connection, press the Escape key.

Default Answer Profile

The Netopia R3100 ISDN Router can answer calls as well as initiate them. To answer calls, the Netopia R3100 uses a Default Answer Profile. The Default Answer Profile controls how incoming calls are set up, authenticated, filtered, and more.

How the Default Answer Profile works

The Default Answer Profile works like a guard booth at the gate to your network: it scrutinizes incoming calls. Like the guard booth, the Default Answer Profile allows calls based on a set of criteria that you define.

The main criterion used to check calls is whether they match one of the Connection Profiles already defined. If PAP or CHAP authentication is being used, the default profile checks that the incoming call's name and password/secret match the receive name and password/secret of a Connection Profile. If PAP or CHAP is not being used, an incoming call is matched to a Connection Profile using the remote network's IP address (that is, the caller is defined as the destination of a particular connection profile).

If an incoming call is matched to an existing Connection Profile, the call is accepted. All of that Connection Profile's parameters, except for authentication, are adopted for the call.

You could set up the Default Answer Profile to allow calls in even if they fail to match a Connection Profile. Continuing the guard booth analogy, this would be like removing the guards or having them wave all calls in, regardless of their source.

If an incoming call is not required to match a connection profile, and fails to do so, it is accepted as a standard IP connection. Accepted, unmatched calls adopt the call parameter values set in the Default Answer Profile.

To determine the call parameter values that unmatched calls will adopt, customize the Default Answer Profile parameters in the Default Answer Profile screen.

Customizing the default profile

You can customize the Netopia Router's default profile in the Default Answer Profile screen under the WAN Configuration menu.

```
┌──────────┐          ┌──────────────┐          ┌────────────────┐
│  Main    │ ───────▶ │     WAN      │ ───────▶ │ Default Answer │
│  Menu    │          │Configuration │          │    Profile     │
└──────────┘          └──────────────┘          └────────────────┘
```
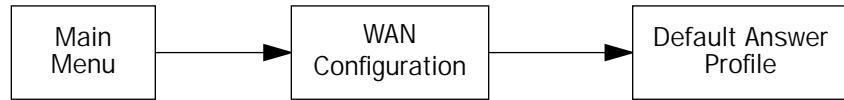
1. Select **Default Answer Profile** in the WAN Configuration screen. Press Return. The Default Profile screen appears.

```
                        Default Answer Profile

            Calling Number Authentication...   Preferred
            Force 56k on Answer:               No

            Must Match a Defined Profile:      Yes




            PPP Authentication...              PAP
            Bandwidth Allocation...            BAP




     Configure values which may be used when receiving a call in this screen.
```

2. To enable CNA-authentication, select **Calling Number Authentication** in the Default Answer Profile screen and choose one of the following settings:

   Ignored: Calling Number Authentication (CNA) is not in effect.

   Preferred: This is the default setting. Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the call proceeds as usual and the caller may still connect successfully. Use this setting if you expect to receive both regular and CNA-authenticated calls.

   Required: Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the Netopia R3100 disconnects the caller. Use this setting if you require all calls to be CNA-authenticated.

   Calling Number Authentication (CNA), is an application of CallerID. It is a method of verifying that an incoming call is originating from an expected site. Using CNA, you can increase the security of your network by requiring that callers not only possess the correct PPP authentication information, but also are calling from a particular physical location.

CNA works by checking the calling number that the Netopia Router receives during the initial setup phase of an incoming call against a set of stored numbers. Each number in the stored set is defined in a specific connection profile. When a match occurs, the incoming call is handled by the connection profile containing the matched number.

Using CNA can also provide cost savings because calls are not billed during the CNA phase. With CNA, a caller can set up a connection to the Netopia R3100 without incurring any charges by accessing a dial-back connection profile. If the caller's rates are higher than those charged to the Netopia R3100's return call, then using CNA has saved the difference.

CNA should be available where CallerID services are available. You will need to consult with your telephone service provider to find out if your line is provisioned for CallerID compliant with Bellcore specifications.

Also note that if the calling side has instructed the phone company to block delivery of its caller ID, the answering side will not be able to authenticate.

Notes:

■   If your line does not support the appropriate service, CNA may not work properly.

■   Certain European switch types do not pass a leading zero (0) in a directory number. If a caller is initiating a call from a number with a leading zero, and you have CNA set to include the leading zero, the connection may fail because the intervening telephone switch dropped the leading zero, and the calling number mismatches your entry. A workaround would be not to use the leading zero in your CNA Validation Number entry in the Telco Options screen. See the Telco Options screen on

3. To force a call to be answered at 56K, toggle **Force 56K on Answer** to **Yes**. Otherwise, the default will remain 64K.

4. To force incoming calls to match connection profiles, select **Must Match a Defined Profile** and toggle it to **Yes**. Incoming calls that cannot be matched to a connection profile are dropped. To allow unmatched calls to be accepted as standard IP or IPX connections, toggle **Must Match a Defined Profile** to **No**.

If **Must Match a Defined Profile** is set to **Yes**, the answer profile only accepts calls that use the same authentication method defined in the **Authentication** item. If PAP or CHAP are involved, the caller must have a name and password or secret that match one of the connection profiles. The caller must obtain these from you or your network administrator before initiating the call.

For example, if **Must Match a Defined Profile** is set to **Yes**, and **Authentication** is set to **PAP**, then only incoming calls that use PAP and match a connection profile will be accepted by the answer profile.

If authentication in the Default Answer Profile is set to CHAP, the value of the **CHAP Challenge Name** item must be identical to the value of the **Send Host Name** item of the Connection Profile to be matched by the caller.

If **Must Match a Defined Profile** is set to **No**, **Authentication** is assumed to be **None**, even if you've set it to **PAP** or **CHAP.** The answer profile uses the caller's IP address to match a connection profile. However, the answer profile cannot discover a caller's subnet mask; it assumes that the caller is *not* subnetting its IP address:

Class A addresses are assumed to have a mask of 255.0.0.0

Class B addresses are assumed to have a mask of 255.255.0.0

Class C addresses are assumed to have a mask of 255.255.255.0. Class C address ranges are generally the most common subnet allocated.

If a remote network has a non-standard mask (that is, it uses subnetting), the only way for it to successfully connect to the Netopia Router is by matching a connection profile. In other words, you will have to set up a connection profile for that network.If **Must Match a Defined Profile** is set to **No**, you can also set the following parameters for accepted calls that do not match a connection profile:

Call acceptance scenarios

The following are a few common call acceptance scenarios and information on how to configure the Netopia R3100 for those purposes.

- To accept all calls, regardless of whether they match a connection profile:

    - Toggle **Must Match a Defined Profile** to **No**.

- To only accept calls that match a connection profile through use of a name and password (or secret):

    - Toggle **Must Match a Defined Profile** to **Yes**, *and*

    - Set **Authentication** to **PAP** or **CHAP**.

    Note: The authentication method you choose determines which connection profiles are accessible to callers. For example, if you choose PAP, callers using CHAP or no authentication will be dropped by the answer profile.

- To allow calls that *only* match a connection profile's remote IP and/or IPX address:

    - Toggle **Must Match a Defined Profile** to **Yes**, *and*

    - set **Authentication** to **None**.

- To not allow *any* incoming calls to connect to the Netopia Router:

    - Toggle **Must Match a Defined Profile** to **Yes**, *and*

    - Set the **Dial** option in the Telco Options screen of every connection profile to **Dial Out Only**

5. If you select **Bandwidth Allocation**, you can select a value from a pop-up window. Supported options are Off, Auto, MP+, or BAP. The Bandwidth Allocation setting will apply to all answered calls.

    Note: The **Bandwidth Allocation** default is BAP. You should only choose one of the other options if you are specifically advised to do so by your ISP or administrator.

Chapter 11

IP Setup and Network Address Translation

The Netopia R3100 uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the router to route IP traffic. You also learn how to configure the router to serve IP addresses to hosts on your local network.

Netopia's SmartIP features IP address serving and Network Address Translation. For a detailed discussion of Network Address Translation, see Appendix F, "Understanding Netopia NAT Behavior." This chapter describes how to use the Network Address Translation feature of SmartIP.

Note: When you configured your Netopia R3100 using SmartStart, Network Address Translation was enabled by default. You have the option of disabling it, if you wish. This is done through the System Configuration screens using Console-based Management.

This section covers the following topics:

■   "Network Address Translation features" on page 11-1

■   "Using Network Address Translation" on page 11-3

■   "IP setup" on page 11-6

■   "IP address serving" on page 11-16

Network Address Translation allows communication between the LAN connected to the Netopia R3100 and the Internet using a single IP address, instead of a routed account with separate IP addresses for each computer on the network.

Network Address Translation also provides increased security by hiding the local IP addresses of the LAN connected to the Netopia R3100 from the outside world.

With SmartIP, the setup is simpler, so Internet service providers typically offer dial-up accounts supporting Network Address Translation at a significant cost savings.

Network Address Translation features

■   NAT is selectable on a per connection basis, optionally allowing real addresses to be used for intranet connections and proxied addresses to be used for Internet connections.

■   The NAT user can use any combination of proxied and unproxied addresses simultaneously on the available Telco channels. For instance, one unproxied address connection profile can be used to connect to a central office, while another proxied address connection profile can simultaneously connect the user's Netopia R3100 and LAN to the Internet.

■   The single proxy address is acquired at connection time from the answering side. The address can be assigned by the remote router from either a dynamic pool of addresses or a fixed, static address.

■   Static NAT (Network Address Translation) Security is made simpler and more reliable by only having to firewall one IP address and by obscuring the internal network structure from the Internet.

Network Address Translation works by remapping the source IP address of traffic from the LAN to a single static or dynamically assigned IP address shown to the remote side of the router.

HOW NAT WORKS

With NAT

ISP*

192.168.1.100
192.168.1.102
192.168.1.103

163.167.132.1

192.168.1.104
192.168.1.105
192.168.1.106

Without NAT

163.167.132.1
163.167.132.2
163.167.132.3

163.167.132.1
163.167.132.2
163.167.132.3
163.167.132.4
163.167.132.5
163.167.132.6

163.167.132.4
163.167.132.5

163.167.132.6
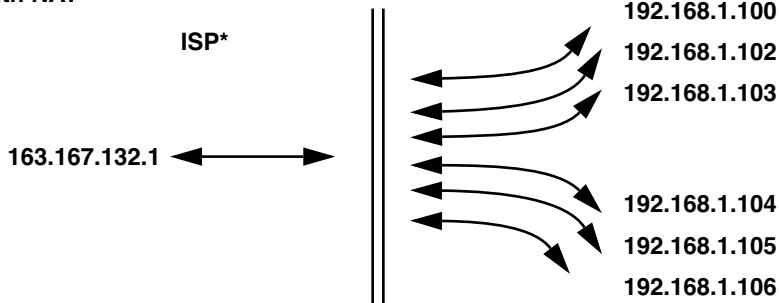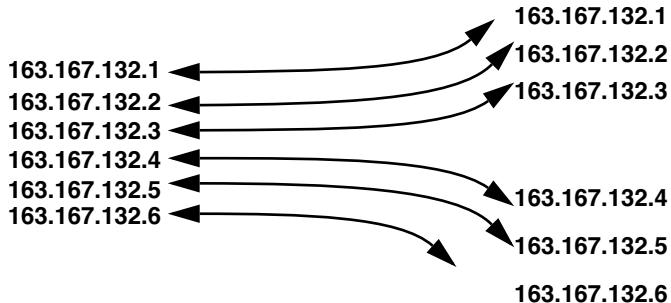
*or corporate intranet router

The feature can be implemented on a per Connection Profile basis. The network router can use two or more Connection Profiles simultaneously to connect to two or more networks. Each profile may have Network Address Translation enabled.

When Network Address Translation is enabled, the Netopia R3100 can either use a statically assigned IP address, or one dynamically assigned each time the router connects to the ISP. While a dynamically assigned IP address offers the ISP more flexibility, it does have an important limitation. The router will require a static IP address to support Web, FTP, or other services available to the WAN. To support these services with Network Address Translation enabled, a service can only be associated with one machine on the LAN.

When connected to the Internet or some other large network using Network Address Translation, the individual machines on your LAN are not directly accessible from the WAN. Network Address Translation provides an inherently secure method of connection to the outside world.

Using Network Address Translation

The following procedure describes how to use Network Address Translation.

1. Pick a network number for your local network (referred to as the internal network). This can be any IP address range you want. The Netopia R3100 ISDN Router has a default IP address of 192.168.1.1. You may choose to change this address to match a pre-existing addressing scheme. For this example, we will use 10.0.0.0.

   Note: The outside world (the external network) will not see this network number.

2. Using the internal network number, assign addresses to the local nodes on your LAN. For example, you may assign

   ■ 10.0.0.1 to your Netopia R3100

   ■ 10.0.0.2 to a node running as a World Wide Web server

   ■ 10.0.0.3 to an FTP server

   ■ 10.0.0.4 to a Windows NT PC

   ■ 10.0.0.5 to a Windows 95 PC

   Note: See "Associating port numbers to nodes" on page 11-5.

3. You created a Connection Profile for your ISP when you ran the SmartStart application. In the Connection Profile, you can toggle **Address Translation Enabled** to **Yes** or **No** (Yes to enable NAT) and press Return.

   The Easy Setup Connection Profile is accessible either:

■ from the Easy Setup menu in the Main Menu screen, go to the Next Screen **Connection Profile 1: Easy Setup Profile**

```
              Connection Profile 1: Easy Setup Profile


      Number to Dial:

      Address Translation Enabled:        Yes


      Local WAN IP Address:               0.0.0.0

      Remote IP Address:                  127.0.0.2
      Remote IP Mask:                     255.0.0.0

      PPP Authentication...               PAP
      Send User Name:
      Send Password:



      PREVIOUS SCREEN                  NEXT SCREEN

   Enter the directory number for the remote network connection.
   Enter basic information about your WAN connection with this screen.
```

■ or, from the WAN Configuration menu in the Main Menu screen. Go to the **Display/Change Connection**

Profile screen. You access the Address Translation option from the **IP Profile Parameters** menu.

```
                      IP Profile Parameters


        Address Translation Enabled:            Yes


        Local WAN IP Address:                   0.0.0.0

        Remote IP Address:                      0.0.0.0
        Remote IP Mask:                         255.0.0.0

        Filter Set...
        Remove Filter Set

        Receive RIP:                            Off




    Configure IP requirements for a remote network connection here.

```

Select the **Local WAN IP Address** field. The default address is 0.0.0.0, which allows for dynamic addressing, meaning that your ISP assigns an address each time you connect. However, if you want to use static addressing you may enter a specific address.

4. When your Netopia R3100 connects to the ISP, the remote router assigns your Netopia R3100 an IP address that external users use to communicate with your network.

   The following Quick View screen shows an example where 192.163.100.6 is assigned to the calling Netopia R3100. "NAT" indicates that the address was assigned dynamically by Network Address Translation.

```
                          Quick View            9/3/1998 01:52:29 PM

    Default IP Gateway:  0.0.0.0           CPU Load: 7%   Unused Memory: 612 KB
    Domain Name Server:  192.168.1.10      Call Acct:     Disabled
    Domain Name: None Provided

    ---------------MAC Address--------IP Address-------IPX Address---EtherTalk---
    Ethernet Hub:    00-00-c5-70-03-48  192.168.1.1                   34449:150



                       Current WAN Connection Status
    Profile Name---------Rate--%Use-Remote Address-----Est--More Info-----------
    ISP                  P1    10%  IP 92.163.4.1       Lcl  NAT 192.163.100.6



                           LED Status
    PWR-+-----WAN1------+--CON--AUX--+-----WAN2------+--EN--+--------LEDS--------
        LNK RDY CH1 Ch2   LNK  LNK   LNK RDY CH1 CH2  DATA |  '-'= Off 'G'= Green
      G   -   -   -   -    -    -     -   -   -   -     Y   |  'R'= Red 'Y'= Yellow

```

Internal users can access the Internet as they always do; the external Internet, however, views all traffic from the internal network as originating from 192.163.100.6. Similarly, all traffic your network receives is addressed to 192.163.100.6.

Associating port numbers to nodes

When an IP client, such as a Netscape Navigator or Microsoft Internet Explorer, wants to establish a session with an IP server, such as a Web server, the client machine must know the IP address to use and the TCP service port where the traffic is to be directed.

For example, a Web browser will locate a Web server by using a combination of the IP address and TCP port that the client machine has set up.

Just as an IP address specifies a particular computer on a network, ports are addresses that specify a particular service in a computer. There are many universally agreed-upon ports assigned to various services. For example:

■   Web servers typically use port number 80

■   All FTP servers use port number 21

■   Telnet uses port number 23

■   SNMP uses port number 161

To help direct incoming IP traffic to the appropriate server, the Netopia R3100 lets you associate these and other port numbers to distinct IP addresses on your internal LAN using Exported Services. See "IP setup" on page 11-6 for details.

Using multiple Connection Profiles

You can enable Network Address Translation on one connection profile, disable it on another, and use the two profiles simultaneously. The profiles might have the following attributes:

■   A profile with Network Address Translation disabled connects to your branch or main office. Your company network administrator has assigned you a local IP address range that is consistent with the address space assigned to your company so that you seamlessly integrate when connected. The remote IP address and mask for this profile define only the company's address space, so that the only IP traffic you send over this connection is for hosts and servers within your company.

■   A Network Address Translation profile connects to the Internet via an ISP. Even though the ISP assigns you a dynamic address each time you connect, there will be no address space conflict, since Network Address Translation hides the corporate address you use locally. You enter the ISP's remote IP address as your default IP gateway so that any IP traffic not intended for your corporate intranet will be directed to the ISP.

Network Address Translation guidelines

Observe the following guidelines when using Network Address Translation.

■   The router can export just one local IP address per TCP port, so you can have just one machine available for a given service, such as one FTP server. However, some services, such as Web servers (www-http servers), allow you to change the TCP port on both the server and client. With two different TCP ports

exported, you can have Web servers on two different IP hosts.

■ If you will be using multiple Connection Profiles, define the remote IP address of the most accessible profile, such as that for your ISP, to the default IP gateway in the TCP/IP settings on users' workstations. That way, IP traffic not intended specifically for any of the remote networks will be routed through this "preferred" profile.

■ Associate your primary Domain Name Server (DNS) with whichever profile is more accessible. If you choose for neither profile to be "dial-on-demand", you may associate a secondary DNS with the other profile. See "IP setup," below, for more information on these settings.

IP setup

```
┌──────────┐      ┌──────────────┐      ┌──────────────┐      ┌──────────┐
│   Main   │ ───▶ │    System    │ ───▶ │   Network    │ ───▶ │ IP Setup │
│   Menu   │      │ Configuration│      │  Protocols   │      │          │
│          │      │              │      │    Setup     │      │          │
└──────────┘      └──────────────┘      └──────────────┘      └──────────┘
```

The IP Setup options screen is where you configure the Ethernet side of the Netopia R3100. The information you enter here controls how the Router routes IP traffic.

Consult your network administrator or Internet Service Provider to obtain the IP setup information (such as the Ethernet IP Address, Ethernet Subnet Mask, Default IP Gateway and DNS Server IP Address) you will need before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia R3100 is reset.

To go to the IP Setup options screen, from the Main Menu select System Configuration and then select **Network Protocols Setup** and then select **IP Setup**.

Note: If you have completed SmartStart or Easy Setup, the information you have already entered will appear in the IP Setup options screen.

```
                           IP Setup


        Ethernet IP Address:                    192.168.1.1
        Ethernet Subnet Mask:                   255.255.255.0

        Default IP Gateway:                     0.0.0.0

        Primary Domain Name Server:             2.0.34.194
        Secondary Domain Name Server:           0.0.0.0
        Domain Name:                            titanic.com

        Exported Services...

        Receive RIP:                            Off
        Transmit RIP:                           Off

        Static Routes...



   Set up the basic IP attributes of your Netopia in this screen.
```

Follow these steps to configure IP Setup for your Netopia R3100:

■   Select **Ethernet IP Address** and enter the IP address for the Netopia R3100's Ethernet port.

■   Select **Ethernet Subnet Mask** and enter the subnet mask for the Ethernet IP Address that you entered in the last step.

■   Select **Default IP Gateway** and enter the IP address for a default gateway. This can be the address of any major router accessible to the Netopia R3100.

    A default gateway should be able to successfully route packets when the Netopia R3100 cannot recognize the intended recipient's IP address. A typical example of a default gateway is the ISP's router.

■   Select **Primary Domain Name Server** and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, robin.hood.com) to the IP addresses actually used by IP routers (for example, 163.7.8.202).

■   If a secondary DNS server is available, select **Secondary Domain Name Server** and enter its IP address. The secondary DNS server is used by the Netopia R3100 when the primary DNS server is inaccessible. Entering a secondary DNS is useful but it is not necessary.

■   Select **Domain Name** and enter your network's domain name (for example, netopia.com). Entering a Domain Name is strongly recommended.

■   Select **Exported Services.** The Exported Services screen appears with three options, **Show/Change Exports**, **Add Export,** and **Delete Export**.
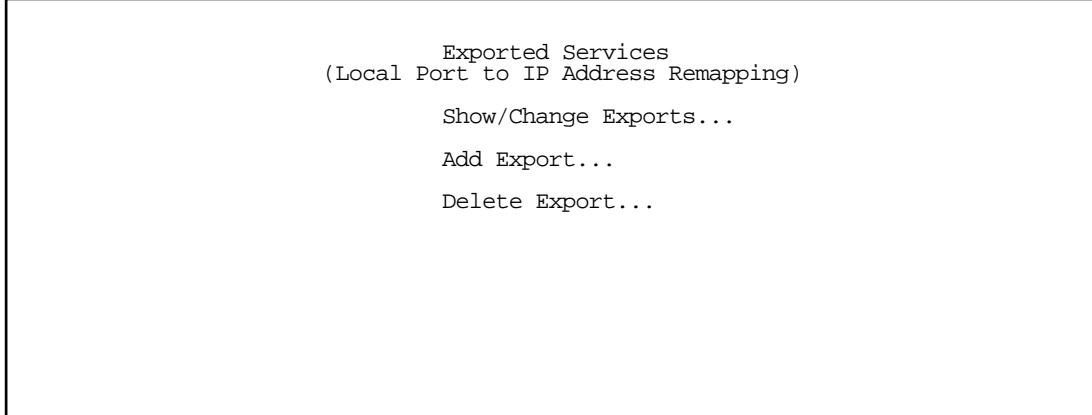
```
                        Exported Services
                (Local Port to IP Address Remapping)

                    Show/Change Exports...

                    Add Export...

                    Delete Export...
```

■   Select **Add Export**. The Add Exported Service screen appears.

```
                      Add Exported Service

              Service...

              Local Server's IP Address:      0.0.0.0

              ADD EXPORT NOW                  CANCEL
```
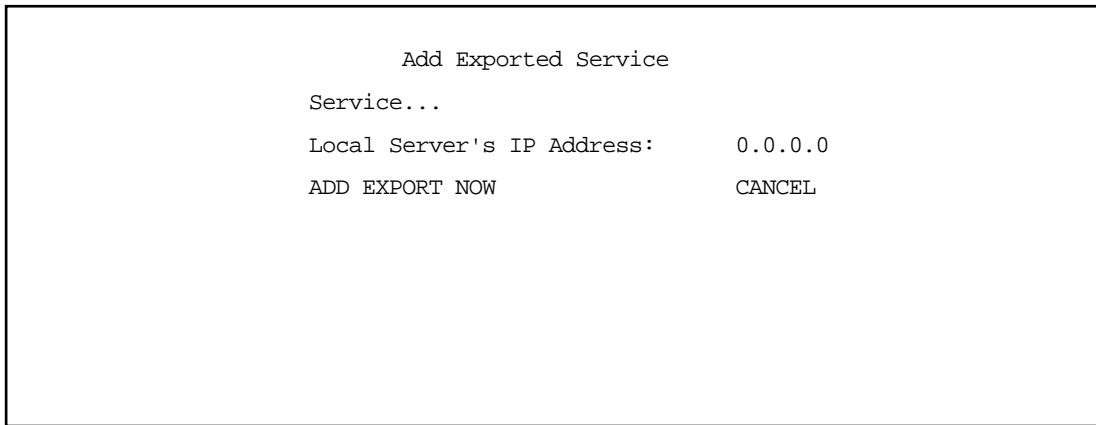
■   Select **Service**. A pop-up menu of services and ports appears.

```
                      Add Exported Service
                                      +-Type------Port--+
                                      +-----------------+
              Service...              | ftp        21   |
                                      | telnet     23   |
                                      | smtp       25   |
              Local Server's IP Address: | tftp    69   |
                                      | gopher     70   |
                                      | finger     79   |
                                      | www-http   80   |
                                      | pop2       109  |
                                      | pop3       110  |
                                      | snmp       161  |
                                      | timbuktu   407  |
                                      | pptp       1723 |
                                      | irc        6667 |
                                      | Other...        |
                                      +-----------------+



              ADD EXPORT NOW                  CANCEL
```

5.   Select any of the services/ports and press Return to associate it with the address of a server on your local area network. For example, if we select **www-http 80**, press Return, and type **10.0.0.2**. The Netopia R3100 will then redirect any incoming traffic destined for a Web server to address 10.0.0.2.

Some services such as Timbuktu require the export of multiple TCP ports. When you associate Timbuktu with a local server (or Timbuktu host) all of the major Timbuktu services are exported, i.e., Observe, Control, Send, and Exchange. These same ports plus www-http should be exported to support a Netopia Virtual Office site on the LAN.

Note: If the TCP port of a service you wish to use is not listed, you can add it by selecting **Other...**

Press the Escape key when you are finished configuring Exported Services to go back to the IP Setup screen.
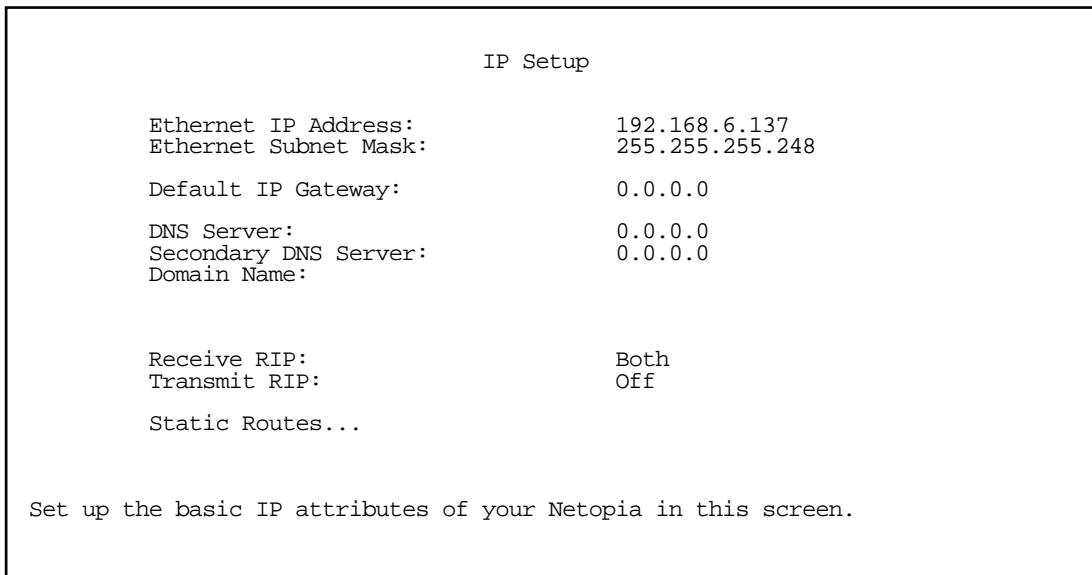
```
                              IP Setup

        Ethernet IP Address:              192.168.6.137
        Ethernet Subnet Mask:             255.255.255.248

        Default IP Gateway:               0.0.0.0

        DNS Server:                       0.0.0.0
        Secondary DNS Server:             0.0.0.0
        Domain Name:



        Receive RIP:                      Both
        Transmit RIP:                     Off

        Static Routes...


   Set up the basic IP attributes of your Netopia in this screen.
```

Follow these steps to configure IP Setup for your Netopia R3100:

■   Select **Ethernet IP Address** and enter the IP address for the Netopia R3100's Ethernet port.

■   Select **Ethernet Subnet Mask** and enter the subnet mask for the Ethernet IP Address that you entered in the last step.

■   Select **Default IP Gateway** and enter the IP address for a default gateway. This can be the address of any major router accessible to the Netopia R3100 such as 127.0.0.2.

    A default gateway should be able to successfully route packets when the Netopia R3100 cannot recognize the intended recipient's IP address. A typical example of a default gateway is the a corporate dial-in or ISP's router.

■   Select **DNS Server** and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, www.netopia.com) to the IP addresses actually used by IP routers (for example, 163.7.8.202).

■   If a secondary DNS server is available, select **Secondary DNS Server** and enter its IP address. The secondary DNS server is used by the Netopia R3100 when the primary DNS server is inaccessible. Entering a secondary DNS is useful but it is not necessary.

■   Select **Domain Name** and enter your network's domain name (for example, netopia.com). Entering a Domain Name is strongly recommended.

■   Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia R3100 needs to recognize. Set to "Both" (the default) the Netopia R3100 will accept information from either RIP v1 or v2 routers. Alternatively, select **Receive RIP** and select **v1** or **v2** from the popup menu. With Receive RIP set to "v1," the Netopia R3100's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to "v2," the

Netopia R3100 will accept routing information provided by RIP packets from other routers that use different subnet masks.

■ If you want the Netopia R3100 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia R3100 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia R3100 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia R3100 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

IP subnets

The IP Subnets screen allows you to configure up to eight Ethernet IP subnets, one "primary" subnet and up to seven secondary subnets, by entering IP address/subnet mask pairs:

```
                    IP Subnets


        IP Address            Subnet Mask
        ----------------      ---------------
 #1:    192.128.117.162       255.255.255.0

 #2:    0.0.0.0               0.0.0.0

 #3:

 #4:

 #5:

 #6:

 #7:

 #8:

```

Note: You need not use this screen if you have only a single Ethernet IP subnet. In that case, you can continue to enter or edit the IP address and subnet mask for the single subnet on the IP Setup screen.

This screen displays up to eight rows of two editable columns, preceded by a row number between one and eight. If you have eight subnets configured, there will be eight rows on this screen. Otherwise, there will be one more row than the number of configured subnets. The last row will have the value 0.0.0.0 in both the IP address and subnet mask fields to indicate that you can edit the values in this row to configure an additional subnet. All eight row labels are always visible, regardless of the number of subnets configured.

■ To add an IP subnet, enter the Netopia R3100's IP address on the subnet in the **IP Address** field in a

particular row and the subnet mask for the subnet in the **Subnet Mask** field in that row.

For example:

```
                        IP Subnets


          IP Address           Subnet Mask
          ----------------     ---------------
    #1:   192.128.117.162      255.255.255.0

    #2:   192.128.152.162      255.255.0.0

    #3:   0.0.0.0              0.0.0.0

    #4:

    #5:

    #6:

    #7:

    #8:
```

■   To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and pressing Return or Enter to commit the change. When a configured subnet is deleted, the values in subsequent rows adjust up to fill the vacant fields.

Note that the subnets configured on this screen are tied to the address serving pools configured on the IP Address Pools screen, and that changes on this screen may affect the IP Address Pools screen. In particular, deleting a subnet configured on this screen will delete the corresponding address serving pool, if any, on the IP Address Pools screen.

If you have configured multiple Ethernet IP subnets, the IP Setup screen changes slightly:

```
                              IP Setup



        Subnet Configuration...

        Default IP Gateway:                192.128.117.163

        Primary Domain Name Server:        0.0.0.0
        Secondary Domain Name Server:      0.0.0.0
        Domain Name:

        Receive RIP:                       Both
        Transmit RIP:                      v2 (multicast)
        Static Routes...

        Address Serving Setup...
        Exported Services...
        Filter Sets...


```
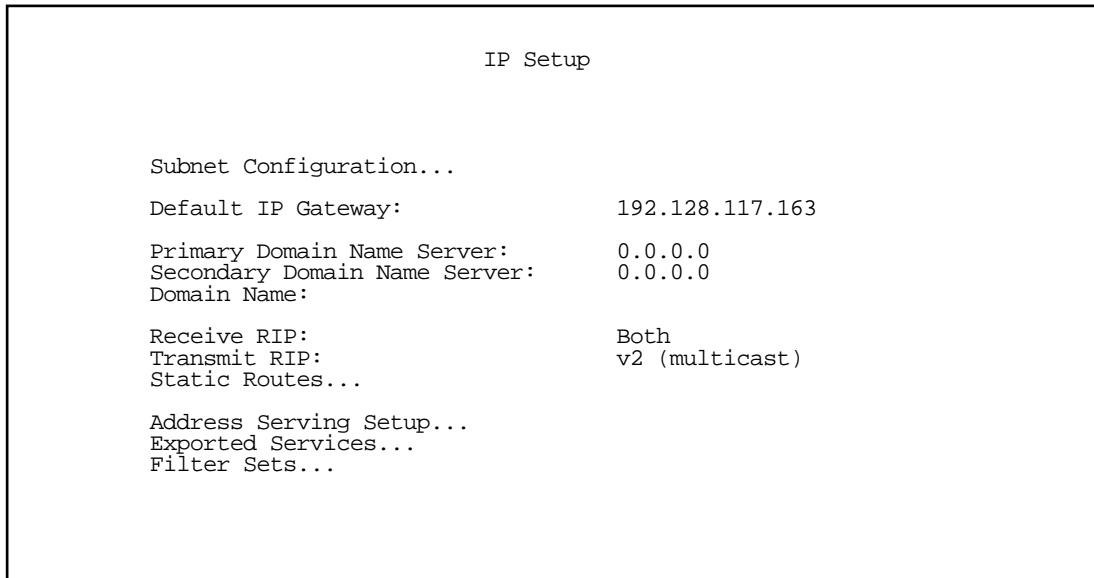
The IP address and Subnet mask items are hidden, and the "Define Additional Subnets..." item becomes "Subnet Configuration...". If you select **Subnet Configuration**, you will return to the IP Subnets screen that allows you to define IP addresses and masks for additional Ethernet IP subnets.

■   Select **Static Routes** to manually configure IP routes. See the following section.

Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Netopia R3100 how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Netopia R3100 (see "IP routing table" on page 14-8).

Static routes are helpful in situations where a route to a network must be used and other means of finding the route are unavailable. For example, static routes are useful when you cannot rely on RIP.

To go to the Static Routes screen, select the **Static Routes** item in the **IP Setup** screen.

```
                        Static Routes

                Display/Change Static Route...

                Add Static Route...

                Delete Static Route...
```

```
Configure/View/Delete Static Routes from this and the following Screens.
```
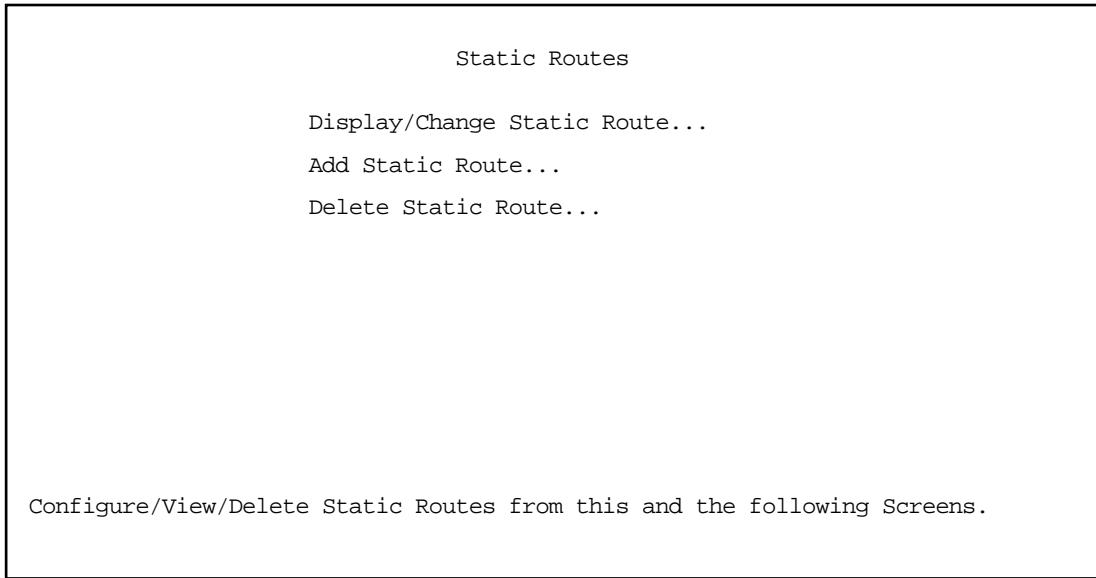
Viewing static routes

To display a view-only table of static routes, select **Display/Change Static Route** in the Static Routes screen.

```
      +-Dest. Network---Subnet Mask-----Next Gateway----Priority-Enabled-+
      +-----------------------------------------------------------------+
      | 0.0.0.0          0.0.0.0          163.176.8.1     Low      Yes   |
      |                                                                  |
      |                                                                  |
      +-----------------------------------------------------------------+
Select a Static Route to modify.
```

The table has the following columns:

Dest. Network: The network IP address of the destination network.

Subnet Mask: The subnet mask associated with the destination network.

Next Gateway: The IP address of the router that will be used to reach the destination network.

Priority: An indication whether the Netopia R3100 will use the static route when it conflicts with information received from RIP packets.

Enabled: An indication whether the static route should be installed in the IP routing table.

Adding a static route

To add a new static route, select **Add Static Route** in the Static Routes screen and go to the Add Static Route screen.

```
                      Add Static Route

        Static Route Enabled:           Yes

        Destination Network IP Address:   0.0.0.0

        Destination Network Subnet Mask:  0.0.0.0

        Next Gateway IP Address:          0.0.0.0

        Route Priority...               High

        Advertise Route Via RIP:        No




        ADD STATIC ROUTE NOW            CANCEL

    Configure a new Static Route in this Screen.
```

- To install the static route in the IP routing table, select **Static Route Enabled** and toggle it to **Yes**. To remove the static route from the IP routing table, select **Static Route Enabled** and toggle it to **No**.

- Be sure to read the rules on the installation of static routes in the IP routing table. See "Rules of static route installation" on page 11-15.

- Select **Destination Network IP Address** and enter the network IP address of the destination network.

- Select **Destination Network Subnet Mask** and enter the subnet mask used by the destination network.

- Select **Next Gateway IP Address** and enter the IP address for the router that the Netopia R3100 will use to reach the destination network. This router does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.

- Select **Route Priority** and choose **High** or **Low**. **High** means that the static route takes precedence over RIP information; **Low** means that the RIP information takes precedence over the static route.

- If the static route conflicts with a connection profile, the connection profile will always take precedence.

- To make sure that the static route is known only to the Netopia R3100, select **Advertise Route Via RIP** and toggle it to **No**. To allow other RIP-capable routers to know about the static route, select **Advertise Route Via RIP** and toggle it to **Yes**. When **Advertise Route Via RIP** is toggled to **Yes**, a new item called **RIP**

Metric appears below **Advertise Route Via RIP**.

With **RIP Metric** you set the number of routers, from 1 to 15, between the sending router and the destination router. The maximum number of routers on a packet's route is 15. Setting **RIP Metric** to **1** means that a route can involve 15 routers, while setting it to **15** means a route can only involve one router.

■ Select **ADD STATIC ROUTE NOW** to save the new static route, or select **CANCEL** to discard it and return to the Static Routes screen.

■ Up to 16 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in System Configuration.

Modifying a static route

To modify a static route, select **Display/Change Static Route** in the Static Routes screen to display a table of static routes.

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see "Adding a static route" on page 11-14).

Deleting a static route

To delete a static route, select **Delete Static Route** in the Static Routes screen to display a table of static routes. Select a static route from the table and press Return to delete it. To exit the table without deleting the selected static route, press the Escape key.

Rules of static route installation

The Netopia R3100 applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

■ The static route's **Next Gateway IP Address** matches the IP address used by a connection profile or the Netopia R3100's Ethernet port.

■ The static route's **Next Gateway IP Address** matches an IP address in the range of IP addresses being distributed by MacIP or DHCP.

■ The static route's **Next Gateway IP Address** is determined to be unreachable by the Netopia R3100.

■ The static route's route information conflicts with a connection profile's route information.

■ The connection profile associated with the static route is set for dial-in connections only, and there is no incoming call connected to that connection profile.

■ The connection profile associated with the static route has a disabled dial-on-demand setting, and there is no current connection using that connection profile.

A static route is already installed in the IP routing table will be removed if any of the conditions listed above become true for that static route. However, an enabled static route is automatically reinstalled once the conditions listed above are no longer true for that static route.

IP address serving

```
┌──────────┐      ┌──────────────┐      ┌──────────────┐      ┌────────────────────────────┐
│   Main   │      │    System    │      │  IP Address  │      │ • Serve DHCP Clients       │
│   Menu   │─────▶│Configuration │─────▶│   Serving    │─────▶│ • Serve BootP Clients      │
│          │      │              │      │              │      │ • Serve Dynamic WAN Clients│
└──────────┘      └──────────────┘      └──────────────┘      │ • Serve Mac IP/KIP Clients │
                                                              └────────────────────────────┘
```

In addition to being a router, the Netopia R3100 is also an IP address server. There are four protocols it can use to distribute IP addresses.

■   The first, called **Dynamic Host Configuration Protocol (DHCP)**, is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are "leased" or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.

■   The second, called **BOOTP** (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BOOTP address assignments are "permanent" since there is no lease renewal mechanism in BOOTP.

■   The third protocol, called **Dynamic WAN**, is part of the PPP/MP suite of wide area protocols used for WAN connections. It allows remote terminal adapters and NAT-enabled routers to be assigned a temporary IP address for the duration of their connection.

■   The fourth protocol, called **MacIP**, is used only for computers on AppleTalk networks. MacIP provides a protocol translation (or gateway) function between IP and AppleTalk as well as an IP address assignment mechanism. Like DHCP, MacIP address assignments are normally temporary, although you may also use static IP addresses with MacIP.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia R3100, and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

To go to the IP Address Serving screen, select **IP Address Serving** in the System Configuration screen and press Return.

```
                          IP Address Serving


        Number of Client IP Addresses:      5
        1st Client Address:                 163.176.56.90

        Serve DHCP Clients:                 Yes
        DHCP NetBios Options...

        Serve BOOTP Clients:                Yes

        Serve Dynamic WAN Clients           Yes

        Serve MacIP/KIP Clients:            Yes
        MacIP/KIP Static Options...


  Configure DHCP, BOOTP, WAN IP, and/or MacIP Address Serving here.
```
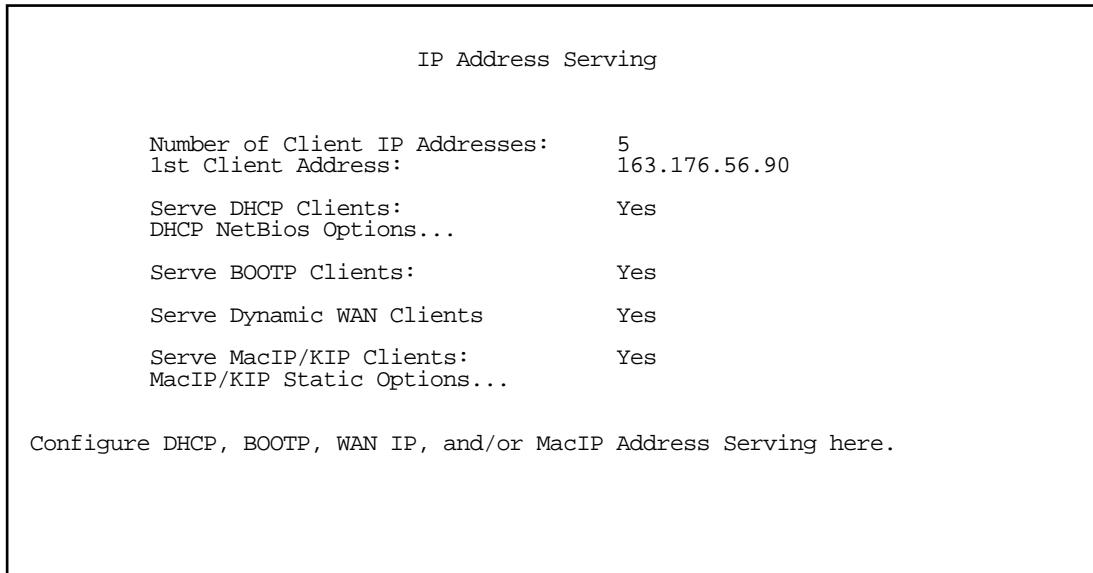
Follow these steps to configure IP Address Serving:

■   If you enabled IP Address Serving either by using SmartStart or in Easy Setup, DHCP, BootP clients, Dynamic WAN clients, and MacIP/KIP clients (if you have the AppleTalk kit installed) are automatically enabled.

■   Select **Number of Client IP Addresses** and enter the total number of contiguous IP addresses that the Netopia R3100 will distribute to the client machines on your local area network.

■   In the screen example shown above, five Client IP addresses have been allocated.

■   Select **1st Client Address** and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may first want to figure out what machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BOOTP, Dynamic WAN, and/or MacIP.

   Note: On a Netopia R3100 the factory default IP Address serving settings are:

   1st Client Address: 192.168.1.3

   Number of Client IP Addresses: unlimited models:100; limited models: number of users minus 1

   (this allows for one static address at 192.168.1.2 for the server)

■   **Example:** Your ISP has given your Netopia R3100 the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet (for more information on understanding IP addressing refer to Appendix E, "Understanding IP Addressing."). Your address range will be from **.137-.143**. In this example you would enter **192.168.6.138** as the 1st client address, as the router itself must have an IP address.

■   To enable DHCP, select **Serve DHCP Clients** and toggle it to **Yes**. DHCP serving is automatic when IP

Address Serving is enabled.

DHCP NetBIOS Options

If your network uses NetBIOS, you can enable the Netopia R3100 to use DHCP to distribute NetBIOS information.

NetBIOS stands for Network Basic Input/Output System. It is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. NetBIOS has been adopted as an industry standard. It offers LAN applications, a variety of "hooks" to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network. To run an application that works with NetBIOS, a non-IBM network operating system or network interface card must offer a NetBIOS emulator. Many vendors either provide a version of NetBIOS to interface with their hardware or emulate its transport layer communications services in their network products. A NetBIOS emulator is a program provided by NetWare clients that allow workstations to run applications that support IBM's NetBIOS calls.

■   Select **Serve NetBIOS Options** and press Return. The DHCP NetBIOS Options screen appears.

```
                    DHCP NetBios Options


        Serve NetBios Type:               Yes
        NetBios Type...                   Type B

        Serve NetBios Scope:              No
        NetBios Scope:

        Serve NetBios Name Server:        No
        NetBios Name Server IP Addr:      0.0.0.0







  Configure DHCP-served NetBIOS options here.

```
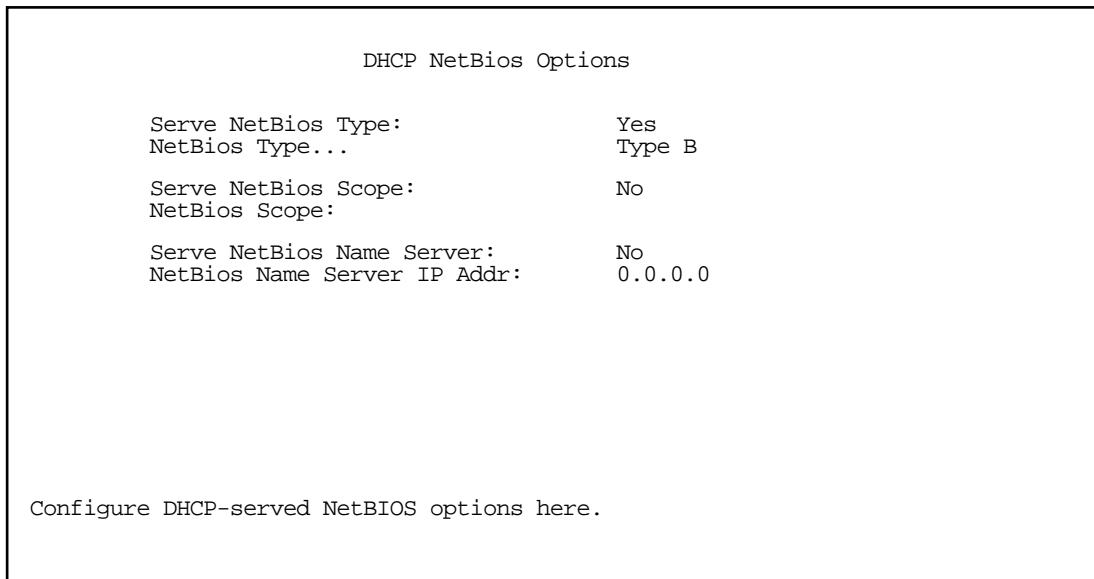
■   To serve DHCP clients with the type of NetBIOS used on your network, select **Serve NetBIOS Type** and

toggle it to **Yes**.

■ From the **NetBIOS Type** pop-up menu, select the type of NetBIOS used on your network.

```
                    DHCP NetBios Options

                                         +--------+
    Serve NetBios Type:                  +--------+
    NetBios Type...                      | Type B |
                                         | Type P |
    Serve NetBios Scope:                 | Type M |
    NetBios Scope:                       | Type H |
                                         +--------+
    Serve NetBios Name Server:           No
    NetBios Name Server IP Addr:         0.0.0.0
```
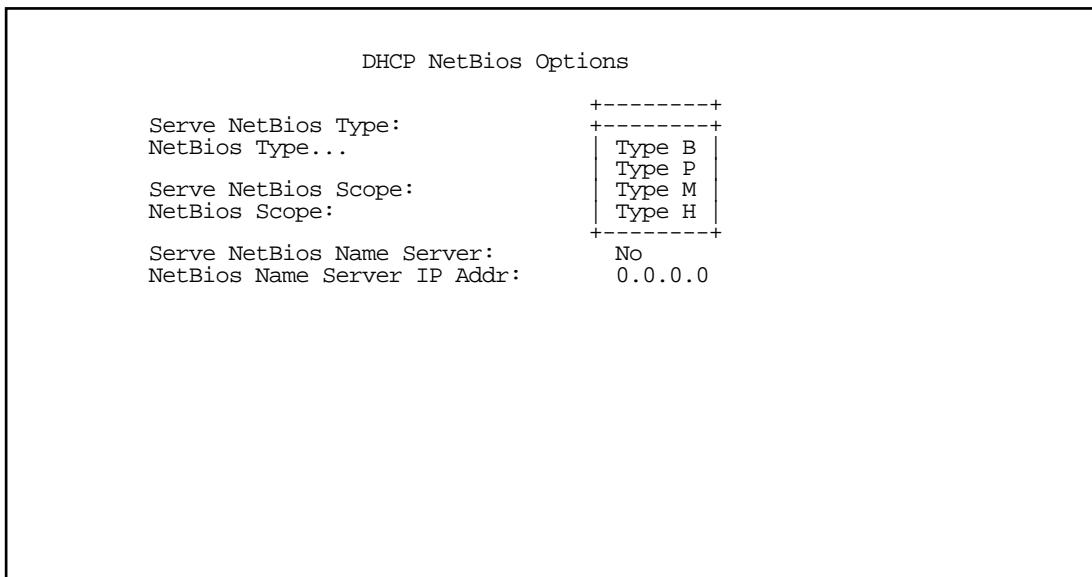
■ To serve DHCP clients with the NetBIOS scope, select **Serve NetBIOS Scope** and toggle it to **Yes**.

Select **NetBIOS Scope** and enter the scope.

■ To serve DHCP clients with the IP address of a NetBIOS name server, select **Serve NetBIOS Name Server** and toggle it to **Yes**.

Select **NetBIOS Name Server IP Address** and enter the IP address for the NetBIOS name server.

You are now finished setting up DHCP NetBIOS Options. To return to the IP Address Serving screen press the Escape key once.

■ To enable BootP's address serving capability, select **Serve BOOTP Clients** and toggle to **Yes**.

Note: Addresses assigned through BOOTP are permanently allocated from the IP Address Serving pool until you release them. To release these addresses, navigate back to the Main Menu, then Statistics & Logs, Served IP Addresses, and **Lease Management**. See .

MacIP (Kip Forwarding) Options

When hosts using AppleTalk (typically those using LocalTalk) are not directly connected to an IP network (usually an Ethernet), they must use a MacIP (AppleTalk-IP) gateway.

The optional Netopia AppleTalk feature enhancement kit provides for this service. A MacIP gateway converts network traffic into the correct format for AppleTalk or IP, depending on the traffic's destination. The MacIP gateway can also distribute IP addresses to AppleTalk computers on the network.

Note: Macintosh computers that have LocalTalk or EtherTalk selected in the MacTCP control panel, or "AppleTalk (MacIP)" selected in the TCP/IP control panel, must use the MacIP gateway to communicate with the Internet or any other IP network. Users should point their MacTCP or TCP/IP control panel to look in the LocalTalk zone for the MacIP server. Macintosh computers that have Ethernet selected in the MacTCP or TCP/IP control panel can do their own AppleTalk-IP conversions.

Setting up MacIP involves choosing MacIP dynamic address serving and then configuring that type. KIP forwarding is simply a method for distributing IP addresses to AppleTalk clients.

To go to the MacIP Setup screen, select **MacIP/KIP Clients** in the IP Address Serving screen from the System Configuration menu.

■ Select **Serve Mac IP/KIP Clients** and toggle to **Yes**, to enable MacIP/KIP address serving capability. This option is automatically enabled if the AppleTalk kit is installed and IP Address Serving is enabled.

■ Select **MacIP/KIP Static Options** and press Return. The MacIP (KIP) Forwarding Setup screen tells the Netopia R3100 how many static addresses to allocate for MacIP/KIP clients. The addresses must fall within the address pool from the previous screen. You will need to enter the number of static MacIP addresses to reserve in this screen.

Note that the address pool IP range will also be listed for your referral in this screen.

```
                        MacIP (KIP) Forwarding Setup


   This screen tells the Netopia how many static addresses to allocate for
   MacIP/KIP clients. The addresses must fall within the address pool from the
   previous screen -- 163.176.56.90 to 163.176.56.94.


          Number of Static Addresses:         0

          First Static Client Address:        0.0.0.0



  Reserve static MacIP addresses for KIP Forwarding here.
```
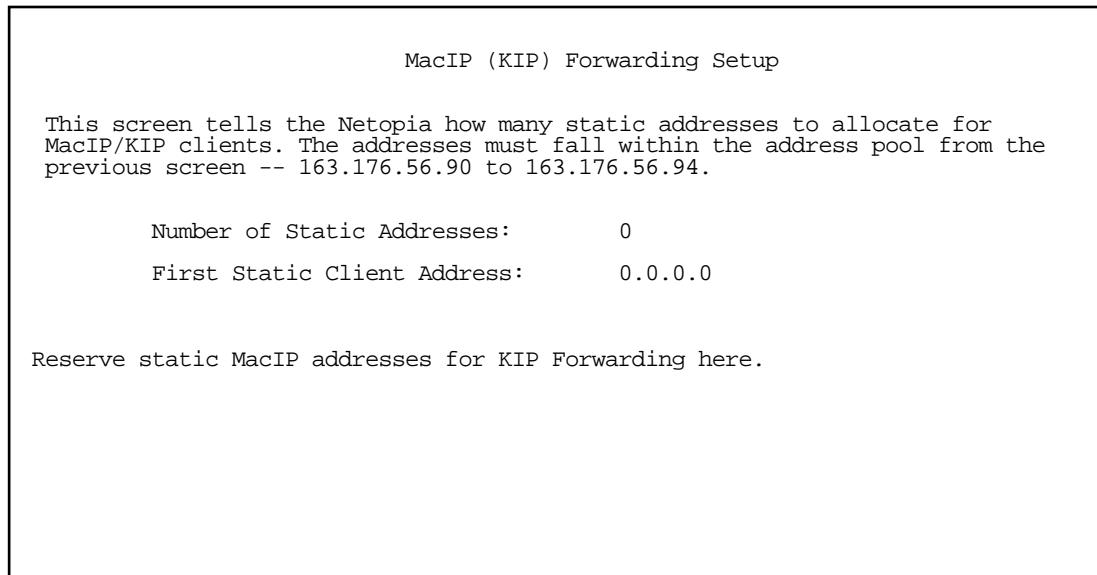
You have finished your IP Setup.

Chapter 12

IPX Setup

Internetwork Packet Exchange (IPX) is the network protocol used by Novell NetWare networks. This chapter shows you how to configure the Netopia R3100 for routing data using IPX. You also learn how to configure the router to serve IPX network addresses.

This section covers the following topics:

IPX Features

The Netopia R3100 supports the following IPX features:

- ■   IPX RIP and SAP
- ■   NetBIOS broadcast packet forwarding (IPX type 20)
- ■   IPX packet filtering definable by source and destination IPX address and socket number, for added security
- ■   IPX SAP filtering to aid in optimizing WAN bandwidth
- ■   Dial-on-demand features:
    - ■   Spoofing of IPX keep-alive, SPX, and server serialization packets
    - ■   Configurable RIP/SAP timers on connection profiles

IPX Definitions

This section defines IPX-related protocols such as RIP, SAP and NetBIOS, in addition to other related terms. See the next section for setup instructions.

Internetwork Packet Exchange (IPX)

IPX is a datagram, connectionless protocol that Novell adapted from Xerox Network System's (XNS) Internet Datagram Protocol (IDP). IPX is dynamically routed, and the routing architecture works by "learning" network addressing automatically.

IPX address

An IPX address consists of a network number, a node number, and a socket number. An IPX network number is composed of eight hexadecimal digits. The network number must be the same for all nodes on a particular physical network segment. The node number is composed of twelve hexadecimal digits and is usually the hardware address of the interface card. The node number must be unique inside the particular IPX network. Socket numbers correspond to the particular service being accessed.

Socket

A socket in IPX is the equivalent of a port in TCP/IP. Sockets route packets to different processes within a single node. Novell has reserved several sockets for use in the NetWare environment:

Field Value	Packet Type	Description
00h	Unknown Packet Type	Used for all packets not classified by any other type
01h	Routing Information Packet	Unused for RIP packets
04h	Service Advertising Packet	Used for SAP packets
05h	Sequenced Packet	Used for SPX packets
11h	NetWare Core Protocol Packet	Used for NCP packets
14h	Propagated Packet	Used for Novell NetBIOS

Routing Information Protocol (RIP)

RIP, which was also derived from XNS, is a protocol that allows for the bidirectional transfer of routing tables and provides timing information (ticks), so that the fastest route to a destination can be determined. IPX routers use RIP to create and dynamically maintain databases of internetwork routing information. See the last section in this chapter for more information on routing tables.

Service Advertising Protocol (SAP)

SAP is a protocol that provides servers and routers with a method to exchange service information. Using SAP, servers advertise their services and addresses. Routers collect this information to dynamically update their routing tables and share it with other routers. These broadcasts keep all routers on the internetwork synchronized and provide real-time information on accessible servers on the internetwork.

The following is a list of common SAP server types:

Unknown	0000h
Print Queue	0003h
File Server	0004h
Job Server	0005h
Print Server	0007h
Archive Server	0009h
Remote Bridge Server	0024h
Advertising Print Server	0047h
Reserved Up To	8000h

NetBIOS

NetBIOS is a protocol that performs tasks related to the Transport and Session layers of the OSI model. It can operate over IPX, using a special broadcast packet known as "IPX Packet type 20" to communicate with IPX NetBIOS servers.

IPX Spoofing

The Netopia R3100 has several IPX features designed to restrict the traffic on the dial-up link when the unit is not sending or receiving IPX data. When the link is idle and a user is logged into a Novell server, the server will send "keep alive" packets to ensure the user is still there. If the link is idle, the "keep alive" packets will be sent back to the server by the locally connected Netopia R3100 as though they came back from the user without bringing up the dial-up link.

Similarly, "SPX keep alive" packets are treated in this manner. IPX RIP, and SAP messages will not be sent if the link is down. Together these features enable the user to remain connected to a Novell server or SPX peer without bringing up the dial-up link, except to send and receive actual user data.

IPX setup

Main Menu → System Configuration → Network Protocols Setup → IPX Setup

The IPX Setup screen is where you configure the Ethernet side of the Netopia R3100. The information you enter here controls how the Router routes IPX traffic.

Consult your network administrator for the IPX setup information you will need before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia R3100 is reset.

To go to the IPX Setup screen, from the Main Menu select System Configuration and then select **Network Protocols Setup** and then select **IPX Setup**.

```
                              IPX Setup
          IPX Routing:                            Off

          Ethernet Encapsulation...               802.3
          Ethernet Network Address:               00000000

          Ethernet Path Delay:                    1
          Ethernet NetBios Forwarding:            No
          Ethernet Inbound SAP Filter Set...      <<NONE>>


          Default Gateway Address:                00000000

          Filters and Filter Sets...

          IPX Wan Pool Base Address               00000000



    Return/Enter accepts * Tab toggles * ESC cancels.
    Set up the basic IPX attributes of your Netopia in this screen.
```

1. To enable IPX routing, select **IPX Routing**, toggle it to **On**, and press Return.

2. To change Ethernet encapsulation from the commonly used 802.3 standard, select **Ethernet Encapsulation** and choose a different encapsulation method.

3. Select **Ethernet Network Address** and enter the network address of the IPX network connected to the Netopia R3100's Ethernet port.

   Note: If the Ethernet network address is set to zero, the Router will attempt to learn the address from any configured IPX device on the Ethernet network or from the remote IPX network when a call is established.

4. To change the default path delay, select **Ethernet Path Delay** and enter a value (in ticks). This value is used to determine the port cost of using the Ethernet port in IPX RIP calculations.

5. To enable NetBIOS packet forwarding, select **Ethernet NetBIOS Forwarding** and toggle it to **Yes**. This parameter will determine whether "IPX Packet type 20" packets are forwarded on the Ethernet interface. These packets are used by NetBIOS and some other applications.

6. Select **Ethernet Inbound SAP Filter Set** to filter incoming IPX SAP advertisements on the Ethernet. By attaching an incoming SAP filter on the Ethernet, you can restrict the number of SAP entries learned on a large IPX network to only those required by remote users connecting to the Netopia R3100. An Ethernet SAP filter *must* be used with networks that have so many servers advertised that the Netopia R3100 would otherwise exhaust its internal memory storing server entries.

   To attach a SAP filter set, first define the filter set using the **Filters and Filter Sets** option (see step 8 below). Then select the filter set from the **Ethernet Incoming SAP Filter Set** pop-up menu. To detach the filter set, select **Detach Filter Set**.

7. Select **Default Gateway Address**, and enter the network address of the IPX network to which all packets of unknown destination address should be routed.

Note: The Default Gateway Address is usually set up to match the IPX Address in your network Connection Profile.

8. To configure filters and filter sets, select **Filters and Filter Sets** and go to the IPX filters and filter sets screens. For information on how to configure IPX filters and filter sets, see .

9. Select **IPX Wan Pool Base Address** and enter the first IPX network address to be allocated to requesting IPX WAN clients. The base address you enter must not conflict with other IPX networks assigned to your IPX internet.

IPX routing tables

```
┌──────────┐     ┌──────────────────┐     ┌──────────────────────────┐
│   Main   │ ──▶ │ Statistics & Logs│ ──▶ │ • IPX Routing Table      │
│   Menu   │     │                  │     │ • IPX SAP Bindery Table  │
└──────────┘     └──────────────────┘     └──────────────────────────┘
```

IPX routing tables provide information on current IPX routes and services.

To go to the IPX Routing Table screen, select **IPX Routing Table** in the Routing Tables screen. This table shows detailed information about current IPX network routes.

```
                            IPX Routing Table

 Net Addr-Hops-Ticks-Type--Status-Interface--------------via Router------------
 ---------------------------------SCROLL UP------------------------------------
 00000020   2      3 RIP    Active Ethernet          00000120:00000c465c2f
 00000030   2     12 RIP    Active Ethernet          00000120:00000c465c2f
 00000033   4     14 RIP    Active Ethernet          000000120:00000c465c2f
 00000100   2      7 RIP    Active Ethernet          00000120:00000c465c2f
 00000110   1      1 RIP    Active Ethernet          00000120:00000c465c2f


 -------------------------------SCROLL DOWN----------------------------
 UPDATE




```

To go to the IPX SAP Bindery Table screen, select **IPX SAP Bindery Table** in the Routing Tables screen. This table shows detailed information about available IPX services and their location.

Chapter 13

AppleTalk Setup

This chapter discusses the concept of AppleTalk routing and how to configure AppleTalk Setup for a Netopia R3100 with the AppleTalk kit installed.

AppleTalk support is available as a separate kit for the Netopia R3100 ISDN Router. Order Netopia Part Number TER/AT01. Skip this chapter if you do not have the AppleTalk kit.

This section covers the following topics:

- "Installing AppleTalk" on page 13-1
- "AppleTalk networks" on page 13-2
- "Configuring AppleTalk" on page 13-6

Note: All changes to AppleTalk options require a restart to take effect. On Netopia R3100 ISDN Routers, the AppleTalk kit LocalTalk features require minimum firmware version 4.3.

Installing AppleTalk

The AppleTalk kit (order TER/AT1) consists of hardware and firmware components that you enable on your router in order to connect an AppleTalk network. The AppleTalk cable supplied in the AppleTalk feature expansion kit connects to the Auxiliary port on the Netopia R3100.

Netopia R3100 back panel

Auxiliary connection port
HD-15 (female)
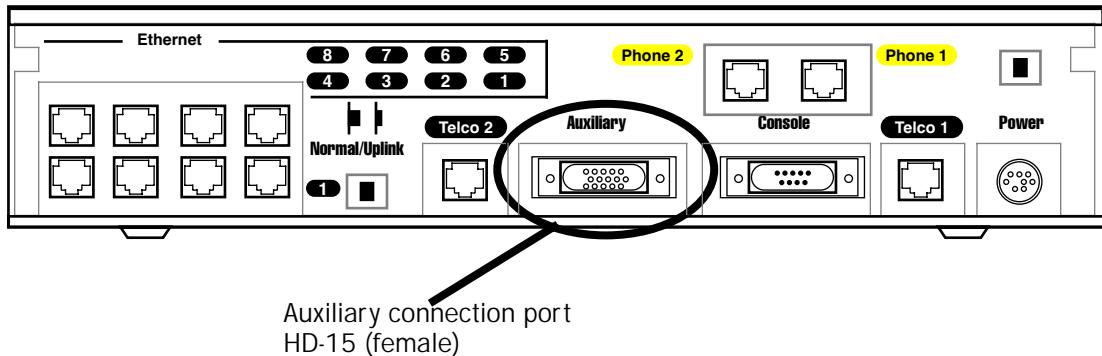
You then enable AppleTalk routing through the Console-based management screens.

To install the AppleTalk features from the Main Menu, go to System Configuration and select **Upgrade Feature Set**.

```
┌─────────────┐      ┌─────────────────┐      ┌─────────────────┐
│    Main     │ ───▶ │     System      │ ───▶ │    Upgrade      │
│    Menu     │      │  Configuration  │      │  Feature Set    │
└─────────────┘      └─────────────────┘      └─────────────────┘
```
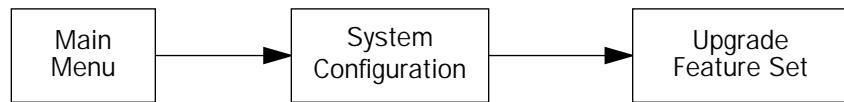
The **Netopia Feature Set Upgrade** screen appears.

```
                    Netopia Feature Set Upgrade

    You may be able to extend the features of your Netopia by purchasing a
    'Software Upgrade'.  For a list of available upgrades, please see the release
    notes that came with your Netopia or visit the Netopia Communications web
    site at www.netopia.com.

    To purchase an upgrade, you must provide your Serial Number, which is:

            xx-xx-xx

    You will receive an Upgrade Key, which you should enter below.

            Upgrade Key:



        UPGRADE NOW                            CANCEL
```

Follow the instructions to enable AppleTalk on your router. Once AppleTalk is enabled, you can configure your network as described in the following sections.

AppleTalk networks

A **network** is a communication system that connects computers to share information using **network services**, such as electronic mail, print spoolers, and file servers. Information is transferred over a cabling system or WAN using a common set of **protocols**. You can think of the cabling system as an organization of cities, streets, and buildings and the protocols as the method of sending letters or packages, as illustrated on the following pages. A **cable** is the physical medium (for example, twisted pair or coaxial) over which information travels from one device to another.

AppleTalk protocol

AppleTalk is a protocol set for local area networks developed by Apple Computer. While initially applied to the **LocalTalk** cabling system for connecting Macintosh computers and LaserWriters, it has been expanded to use other cabling systems, such as Ethernet, as well as the dial-up telephone networks and packet switching systems. LocalTalk was originally known as the AppleTalk Personal Network system.

Each computer or peripheral device (printer, client, file server) connected to a network is called a **node** and has a unique **node address**, which can be any number from 1 to 254. Whenever you open the Chooser or any application that communicates with other computers on your network, your application compiles a list of all node names and addresses. All you see are the names --- for example, "Paul'sMac," "TechSportsWriter," or "2nd Floor AppleShare" --- but your application also knows the node addresses of all these devices.

When you send information, commands, or requests to a printer, server, or another workstation, your application formats the information into units known as **packets**. It then attaches the correct address to the packets and sends them to the AppleTalk software on your computer, which forwards the packets across the network. Packets also include a return address, so the receiver will know where to reply.

If the cabling of your network were a street system, then a node address would correspond to a building's street address. Node addresses are not permanent. Each AppleTalk device determines its node address at startup. Although a Macintosh that is starting up will try to use its previous address, the address will often be different upon restart. This **dynamic node addressing** scheme prevents conflicts when devices are moved between networks and simplifies the administrative tasks of a network. If you have only one network, the node address alone is all the information AppleTalk needs to send a packet from one computer to another.

However, networks can be connected together through **routers**, such as the Netopia R3100, into an **internetwork** (often shortened to **internet**). Because devices on different networks can have duplicate node numbers, AppleTalk tells them apart according to an additional part of their addresses: the **network number**.

The Netopia R3100 assigns a unique network number to each member network. In terms of the city street metaphor, the network number is similar to the name of the street. Putting a network number together with a node number fully specifies the address of a node on an internet.

To make the services on an internet manageable, groups of devices on a network can be grouped into zones. When this is done, selecting a network service (server, etc.) includes choosing a zone from which the service can be selected. Like network numbers, **zone names** are assigned by routers.

A **routing table** is maintained by each AppleTalk router. The table serves as a map of the internet, specifying the path and distance, in hops, between its router and other networks. The routing table is used to determine whether a router will forward a data packet and, if so, to which network.

You can use the information in the AppleTalk routing table to observe and diagnose the Netopia R3100's current connections to other AppleTalk routers. To go to the AT Routing Table screen from the Netopia R3100's console, select **Statistics & Logs** from the Main Menu and then select **AppleTalk Routing Table**.

```
                            AT Routing Table

-Net---Range--Def Zone Name---------Hops-State-Next Rtr Addr.--Pkts Fwded
--------------------------------SCROLL UP------------------------
  1     --      Admin              2    Good  46.131           0
  2     --      AdMan              2    Good  46.131           0
  3     --      Aspirations        2    Good  46.131           0
  4     --      Sales              2    Good  46.131           0
  5     --      Marketing          2    Good  46.131           0
  6     --      Molluscs           2    Good  46.131           1
  7     --      Customer Service   2    Good  46.131           1
  8     --      Telemarketing      2    Good  46.131           0
 10     --      Rio                2    Good  46.131           0
 11     --      Regiment           2    Good  46.131           0
 12     --      Rhinos             2    Good  46.131           0
 16     --      Unique Services    2    Good  46.131           0
*24     27      Aspirations        1    Good  46.131          79
 28     31      Rhinos             1    Good  46.131          15
-------------------------------SCROLL DOWN-----------------------
UPDATE

'*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

A router has multiple communications ports and is capable of forwarding information to other routers and devices on the internet. The router performs packet forwarding, network and device address maintenance, and other administrative functions required by the AppleTalk protocols.

MacIP

When Macintosh computers encapsulate TCP/IP packets in AppleTalk, either because they are on LocalTalk or they are on EtherTalk for administrative reasons, they must use the services of a MacIP gateway. This gateway converts network traffic into the correct format for AppleTalk or IP, depending on the traffic's destination. Setting up MacIP involves enabling the feature and optionally setting up a range of addresses to be static.

See Chapter 8, "IP Setup." for more information on how to set up MacIP and other IP addressing schemes.

AURP

AppleTalk Update-Based Routing Protocol (AURP) allows AppleTalk networks to communicate across an IP network. Your local AppleTalk networks (connected to the Netopia R3100) can exchange data with remote AppleTalk networks that are also connected to an AURP-capable router.

When two networks using AppleTalk communicate with each other through a network based on the Internet Protocol, they are said to be tunneling through the IP network. The Netopia R3100 uses AURP to allow your AppleTalk network to tunnel to designated AppleTalk partner networks, as well as to accept connections from remote AppleTalk networks tunneling to your AppleTalk LAN.

Routers and seeding

To configure AppleTalk networks, you must understand the concept of **seeding**. Seeding is the process by which routers (or more specifically, router ports) agree on what routing information is valid. AppleTalk routers that have been reset, for example, must decide what zones and network numbers are valid before they begin routing. In this case, a router may use the information it has stored, or use information it receives from another router, depending on how it has been configured.

To help ensure agreement between routers on a network, a **seed router** is configured with the correct information, and other routers obtain their information from that router when they are turned on or reset.

Routers commonly use one of three types of seeding procedures: hard seeding, soft seeding, and non-seeding.

Hard seeding: When a router that uses hard seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. If no other routers reply, the router uses the network numbers and zone names specified in its own configuration. If other routers reply, and their information matches the router's own configuration information, the result is the same—the router uses the values in its own configuration. However, if other routers provide network numbers or zone names that conflict with those in the router's configuration, the router disables any of its own ports for which there are conflicts.

Soft seeding: When a router that uses soft seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. If no other routers reply, the router uses the network numbers and zone names specified in its own configuration. If other routers reply, the router uses the information they provide, regardless of whether or not there are conflicts between the information received and its configured information. Once a soft- or hard seeding router begins to route, it can serve as a seed router, providing network number and zone name information to other routers upon request. The default state of the Netopia R3100's AppleTalk ports is soft seeding.

Non-seeding: When a router using non-seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. For any network where no other routers reply, the non-seeding router will not have any active ports until the next reset.

You should set the Netopia R3100's seeding action to work best in your particular network environment. These scenarios may guide you in deciding how to set the router's seeding:

■ If the Netopia R3100 is the only router on your network, you must set it to either hard seeding or soft seeding. The default is soft seeding.

■ If there is another active router on your network, and you want that router to configure the Netopia R3100's EtherTalk or LocalTalk parameters, you can set the Netopia R3100 to non-seeding.

■ If there is another active router on your network, you could set the Netopia R3100 to be soft seeding if you are unsure that the second router would always be available to configure the Netopia R3100's EtherTalk or LocalTalk parameters.

■ If you want the Netopia R3100 to configure the EtherTalk or LocalTalk parameters of other routers on your network, you must set it to hard seeding. In this case, the other routers must be soft seeding or non-seeding, and the Netopia R3100 must already be active when those other routers are rebooted.

■ If you want the Netopia R3100 and all other routers on your network to use only their own configurations, set the Netopia R3100 and all other routers to hard seeding. In this case, any router (including the Netopia R3100) that is rebooted will not begin routing if it detects a routing conflict between itself and any other router. This last scenario could be useful for detecting and locating routing errors on your network.

Configuring AppleTalk

You can configure AppleTalk basic services through the Easy Setup screen in the Main Menu.

```
                        AppleTalk Easy Setup

        AppleTalk Routing:               On

        AppleTalk Zone Name:             Aspirations

        EtherTalk Phase II Enabled:      On
        EtherTalk Net Number (0..65279): 34449




        PREVIOUS SCREEN                          NEXT SCREEN

Return/Enter accepts * Tab toggles * ESC cancels.
Configure basic AppleTalk services here.
```

When you install AppleTalk, EtherTalk Phase II is enabled by default. If you have other AppleTalk routers on your LAN, you can accept all of the defaults and simply enter the AppleTalk Zone Name of the zone your router is attached to.

For additional features, see the following sections.

AppleTalk setup for Netopia R3100s consists of configuring EtherTalk, LocalTalk (available in a future release), and AURP.

EtherTalk Setup

To go to the EtherTalk Setup options screen, select **Network Protocols Setup** and then select **AppleTalk Setup** in the System Configuration screen. Select **EtherTalk Phase II Setup** and press Return.

```
+------------------------------------------------------------------------+
|                                                                        |
|                         EtherTalk Phase II Setup                       |
|                                                                        |
|      EtherTalk Phase II Enabled:     +---------ET II Zone List---------+|
|                                      +--------------------------------+ |
|      Show Zones...                   | Unnamed                        | |
|                                      |                                | |
|      Enter New Zone Name:            |                                | |
|                                      |                                | |
|      Delete Zone Name...             |                                | |
|                                      |                                | |
|      Set Default Zone...             |                                | |
|                                      |                                | |
|      Net Low:                        |                                | |
|      Net Hi:                         |                                | |
|                                      |                                | |
|      Seeding...                      |                                | |
|                                      +--------------------------------+ |
|                                                                        |
|                                                                        |
|  Up/Down Arrow Keys to select, ESC to dismiss.                         |
|                                                                        |
|                                                                        |
+------------------------------------------------------------------------+
```
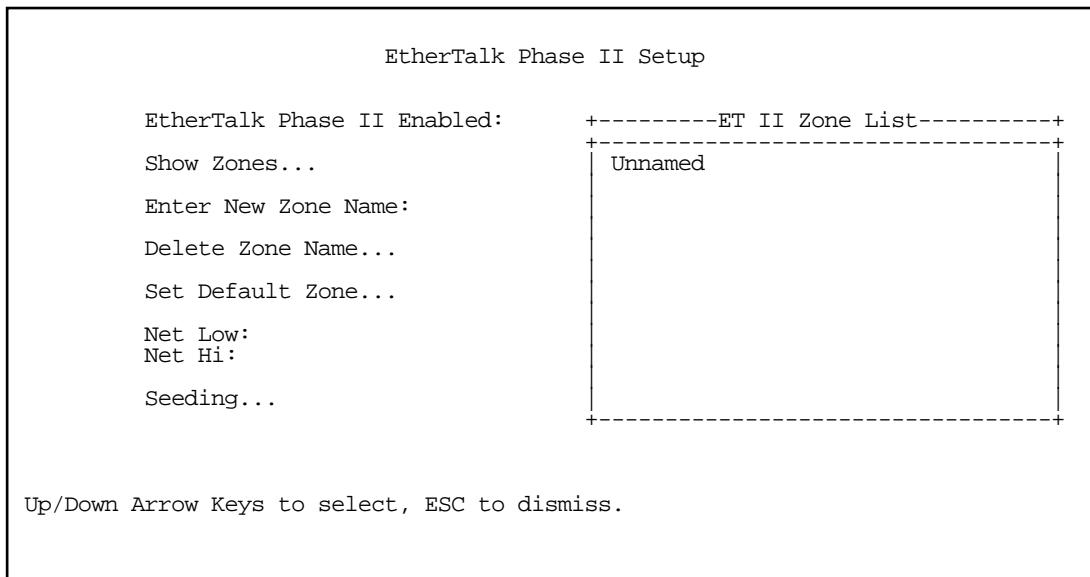
- If you are using EtherTalk Phase II on the Ethernet network connected to Netopia R3100, select **EtherTalk Phase II Enabled** and toggle it to **On**.

- To view the zones available to EtherTalk Phase II, select **Show Zones** and press Return. You can dismiss the list of zones by pressing the Return or Escape key.

- Select **Enter New Zone Name** to enter a new zone name.

  Note: Your EtherTalk network number and zone name must match the values in use on the EtherTalk network.

  If another router is already present on the EtherTalk network that you will be connecting to the Netopia R3100, use the zone names and network numbers used by that router for that EtherTalk network. Otherwise, your EtherTalk network may experience routing conflicts. The Netopia R3100 supports creating up to 32 zone names.

  As an alternative, you can set EtherTalk seeding to soft seeding and let the Netopia R3100 receive the zone name and network number from the other router.

- To remove zones from the list, select **Delete Zone Name** and press Return to see the zones list. Use the Up and Down Arrow keys to select the zone to delete. Press the Return key to delete it and exit the list. Press the Escape key to exit the list without deleting any zones.

- Select **Set Default Zone** to choose a different default zone. This is the zone where the Netopia R3100's EtherTalk Phase II port is visible to other AppleTalk nodes. The default zone is also where new AppleTalk nodes will appear. If you do not set a default zone, the first zone you create will be the default zone.

- You can also set the range of EtherTalk Phase II network numbers. Select **Net Low** and enter the lower limit

of the network number range. Select **Net High** and enter the upper limit of the range.

■   Select the **Seeding** pop-up menu and choose the seeding method for the Netopia R3100 to use (see "Routers and seeding" on page 13-5).

You have finished configuring EtherTalk Phase II.

LocalTalk Setup

Note: For instructions on making the physical connections for LocalTalk, see "Connecting to a LocalTalk network" on page 4-6.

Select **LocalTalk Setup** in the AppleTalk Setup screen and press Return to the LocalTalk Routing Setup screen.

```
                            LocalTalk Setup

        LocalTalk Enabled:              On

        LocalTalk Zone Name:            Unnamed

        LocalTalk Net Number:           33126

        Seeding...                      Soft-Seeding




     Use this screen to set up the LocalTalk Port Routing attributes.


```
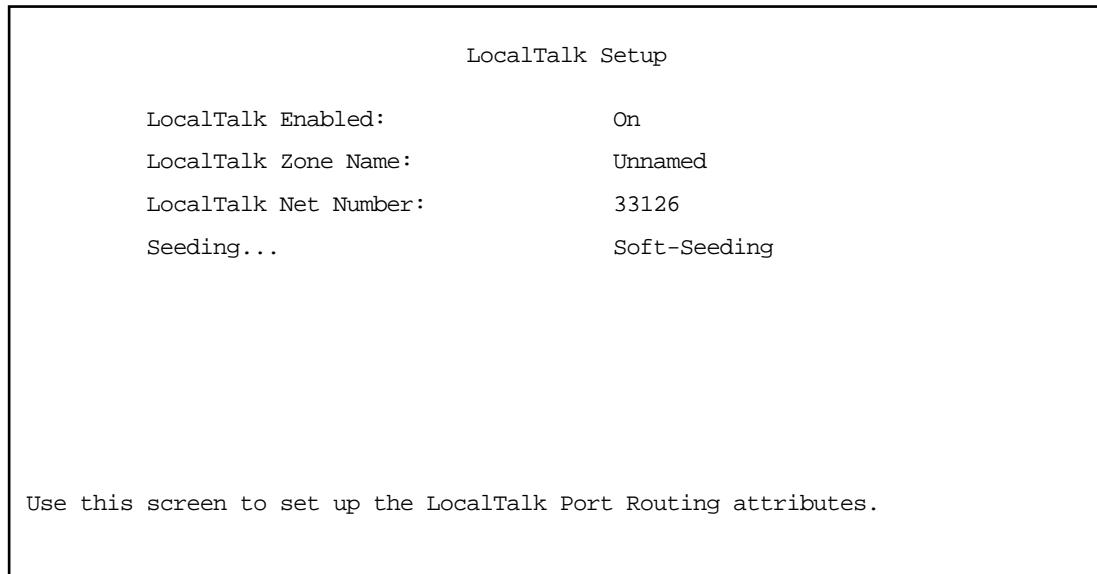
■   If you are using LocalTalk with the Netopia R3100, select **LocalTalk Enabled** and make sure LocalTalk is set to **On,** which is the default.

Note: Since the LocalTalk connector attaches to the Auxiliary port on the router, that port will no longer be available for an external modem.

■   Select **LocalTalk Zone Name** and enter a new or existing zone name.

Note: Your LocalTalk network may already have a zone and network number in place. For the Netopia R3100's LocalTalk port to be part of your LocalTalk network, it must have a network number and zone name that matches the values in use on the LocalTalk network.

If another router is already present on the LocalTalk network that you will be connecting to the Netopia R3100, use the zone name and network number used by that router for that LocalTalk network. Otherwise, your LocalTalk network may experience routing conflicts.

As an alternative, you can set LocalTalk seeding to soft seeding and let the Netopia R3100 receive the zone name and network number from the other router.

■   Select **LocalTalk Network Number** and enter the desired network number.

■   Select **Seeding.** From the pop-up menu, choose the type of seeding for the Netopia R3100's LocalTalk port to use (see "Routers and seeding" on page 13-5).

You have finished configuring LocalTalk.

AURP setup

To set up AURP, select AppleTalk Setup from the Network Protocols screen. Select **AURP Setup** and press Return.

```
+------------------------------------------------------------------------+
|                                                                        |
|                             AURP Setup                                 |
|                                                                        |
|        AURP Enable:                          On                        |
|        Display/Change Partner...                                       |
|        Add Partner...                                                  |
|        Delete Partner...                                               |
|                                                                        |
|        Enter Free Trade Zone Name:                                     |
|        Accept Connections From...            Configured Partners Only  |
|                                                                        |
|        Advanced Options...                                             |
|                                                                        |
|                                                                        |
|   AURP Allows you to connect remote AppleTalk Networks across IP.      |
|                                                                        |
|                                                                        |
+------------------------------------------------------------------------+
```
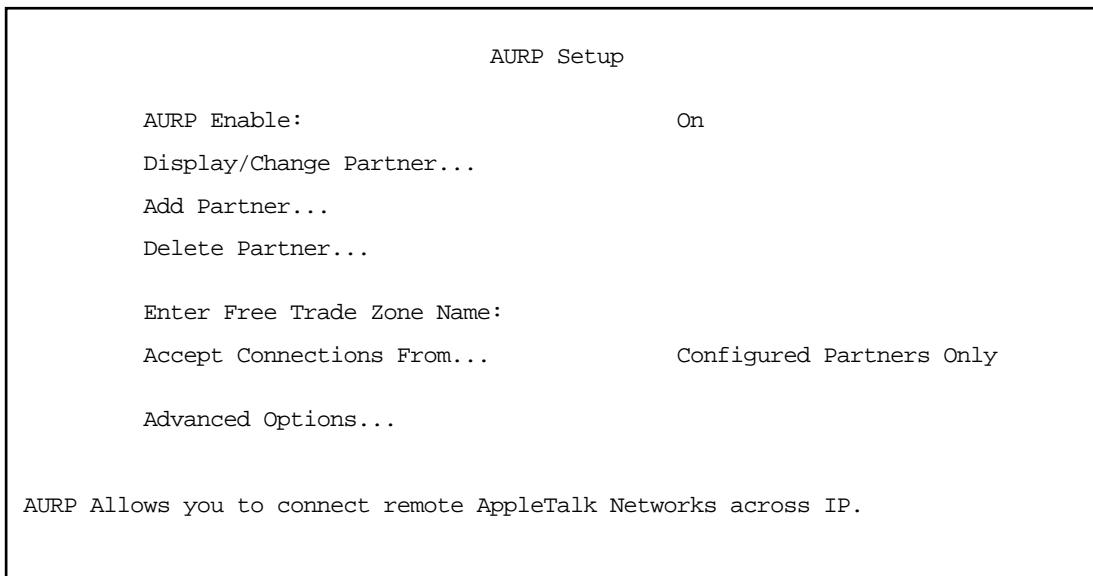
■   To activate AURP and enable connections to and from AURP partners, select **AURP Enable** and toggle it to **On**.

Viewing AURP partners

■   To see a table of existing AURP partners, select **Display/Show Partners** and press Return.

    Note: The Netopia R3100 can define a total of 32 AURP partners.

AURP Free Trade Zone

The Free Trade Zone is an AURP security feature. It allows the Netopia administrator to specify a single AppleTalk zone that will be the only one visible to the remote side for partners that have this option enabled.

Example:

Site A has an AURP tunnel to site B. Both sides have multiple zones defined on the EtherTalk port and a unique zone on their LocalTalk ports. If side A has indicated one of its EtherTalk zones is the Free Trade Zone and has opted to use the Free Trade Zone option for its tunnel to B, then only this Free Trade Zone will show up on side B and only those machines or services in the Free Trade Zone will be accessible to side B. All of side A will be able to see all of side B.

Adding an AURP partner

■   To add a new AURP partner, select **Add Partner** and press Return to go to the Add AURP Partner screen.

```
                            Add AURP Partner


        Partner IP Address or Domain Name:

        Initiate Connection:                No

        Restrict to Free Trade Zone:        No






        ADD PARTNER NOW                     CANCEL
   Enter Information about new Partner.
```
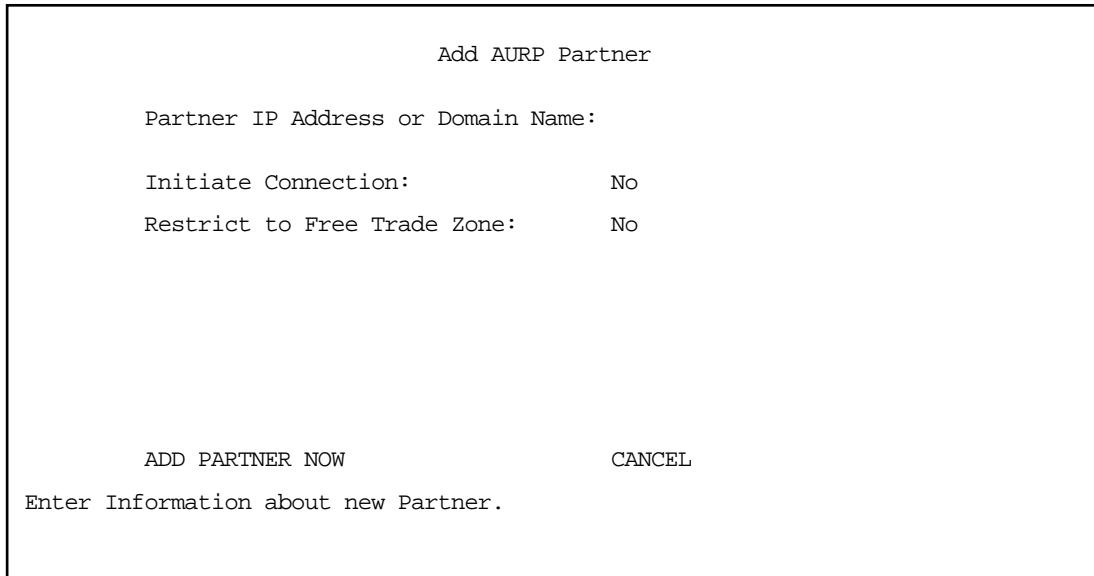
■   Select **Partner IP Address or Domain Name** and enter the new AURP partner's IP address. If you do not know the remote network's IP address, enter its domain name. Domain names are the Internet addresses favored by people (for example, chagall.arts.edu). Domain names are matched to the IP addresses actually used by IP routers (for example, 163.7.8.202).

■   To initiate a connection with an AURP partner, select **Initiate Connection** and toggle it to **Yes**. This will open a connection to the remote AppleTalk network after rebooting.

■   You can choose to restrict this partner to the Free Trade Zone by toggling **Restrict to Free Trade Zone** to **Yes**. See "AURP Free Trade Zone" on page 13-9 for more information.

■   To add the new AURP partner, select **ADD PARTNER NOW**. To discard the new AURP partner, select **CANCEL**.

Modifying an AURP partner

■   To modify an AURP partner, select **Display/Change Partner** in the AURP Setup screen and press Return to display a table of existing partners.

   Use the Up and Down Arrow keys to select a partner, then press Return to go to the Change AURP Partner screen.

Deleting an AURP partner

■ To delete an AURP partner, select **Delete Partner** in the AURP Setup screen and press Return to display a table of existing partners.

Use the Up and Down Arrow keys to select an AURP partner, then press Return to delete it. Press the Escape key to exit without deleting a partner.

Receiving AURP connections

■ To control the acceptance of incoming AURP tunnels, select **Accept Connections From** and choose **Anyone** or **Configured Partners Only** from the pop-up menu. If you choose **Anyone**, all incoming AURP connections will be accepted.

The more secure option is **Configured Partners Only**, which only accepts connections from recognized AURP partners (the ones you have set up).

Configuring AURP Options

In the AURP Setup screen, Select **AURP Options** and go to the AURP Options screen. Using AURP can cause a problem when two networks, one local and one remote, have the same network number. This may cause network routing ambiguities than can result in routing errors.

```
                           AURP Options


        Tickle Interval (HH:MM:SS):          00:00:00
        Update Interval (HH:MM:SS):          00:00:30


        Enable Network Number Remapping:     Yes

        Remap into Range
                From:                        4096
                To:                          32768

        Cluster Remote Networks:             No

        Enable Hop-Count Reduction:          No




 Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

```

■ Select **Tickle Pkt Rqst Interval (HH:MM:SS)** and set the timer to indicate how often a tickle or 'are you still there' packet will be sent to the remote AppleTalk Network.

The AURP tickle timer is a parameter that you can set anywhere between 0 and 100 hours. This parameter tells the AURP partners when to send out an AURP tickle packet. If this value is set to 0, the Netopia R3100 will never send out a tickle packet. Tickle packets verify that the remote router is working. The minimum tickle interval is 90 seconds. The maximum tickle interval setting is 99:59:59 (100 hours), which is the recommendation for small networks.

Raising the tickle packet interval does not ensure that the AURP tunnel is dropped or not brought up. If any application on the local network generates AppleTalk traffic destined for the network at the remote end of the AURP tunnel, the tunnel remains up. For example, if a host on the local network connects to a host on the remote network using remote access software, the AURP tunnel remains up. The AURP tunnel also remains up if a local user selects the Chooser and uses an AppleTalk service that involves a remote zone, such as mounting a remote AppleShare volume.

■   In many AppleTalk internets, individual AppleTalk networks come and go. Routers are designed to notify each other at the end of their **Update Interval** every time there's such a change in the network topology. This will cause the Netopia's WAN link to be brought up. You can opt to minimize what may be unnecessary calls by changing the Update Interval value to some larger value. At the end of this time window if there has been a local AppleTalk network change the Netopia R3100 will call any remote AURP partner and forward the new network information.

■   To enable network number remapping, select **Enable Network Number Remapping** and toggle it to **Yes**.

You should enable network number remapping if you plan on using AURP when connecting to unknown AppleTalk networks. for example when "Accept Connections from Anyone" is enabled. With remapping, the Netopia R3100 will substitute network numbers not used by your network for the numbers of other remote networks. These safe remappings will only be used by local routers on your network; remote routers will not be aware of the remapping.

When network number remapping is enabled, you *must* choose a safe range of network numbers as a destination for the remapping. A safe range of network numbers does not intersect your local AppleTalk network's range of network numbers.

■   To choose a destination range for the remapping, select **From** under **Remap into Range** and enter a starting value. Then select **To** and enter an ending value. Make sure the range you choose is large enough to accommodate all expected incoming AURP network numbers.

■   To improve the efficiency of remapping network numbers into a safe range, select **Cluster Remote Networks** and toggle it to **Yes**. This setting takes any number of remote networks being remapped and causes them to be remapped into a continuous range.

■   To override the AppleTalk maximum limit of 15 hops, select **Enable Hop-Count Reduction** and toggle it to **Yes**. Hosts on a local AppleTalk network will then "see" AppleTalk destinations across the IP tunnel as being only one hop away.

AppleTalk allows a packet up to 15 hops (going through 15 AppleTalk routers) to reach its destination. Packets that must reach destinations more than 15 hops away will not succeed, therefore tunneling from one large AppleTalk network to another could exceed that limit. In such a case, hop count reduction enables full network to network communication.

You have finished configuring AURP.

Chapter 14

Monitoring Tools

This chapter discusses the Netopia R3100's device and network monitoring tools. These tools can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

This section covers the following topics:

Quick View status overview

You can get a useful, overall status report from the Netopia R3100 in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.

```
┌──────────┐        ┌──────────────┐
│   Main   │───────▶│  Quick View  │
│   Menu   │        │              │
└──────────┘        └──────────────┘
```
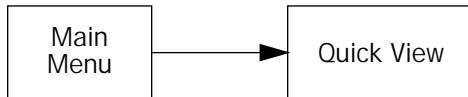
The Quick View screen has three status sections:

■   General status

■   Current WAN Connection Status

■   LED Status

The status sections vary according to the interface of your Netopia R3100.

General status

```
                          Quick View              8/13/1998 03:29:57 PM
Default IP Gateway:  163.176.8.1       CPU Load: 3%     Unused Memory: 646 KB
Domain Name Server:  163.176.4.31      Call Acct:       Disabled
Domain Name: netopia.com

----------------MAC Address--------IP Address-------IPX Address---EtherTalk---
Ethernet Hub:    00-00-c5-70-03-48  192.168.1.1                        24:150



                     Current WAN Connection Status
Profile Name---------Rate--%Use-Remote Address-----Est.-More Info------------



                              LED Status
PWR-+-----WAN1------+--CON--AUX--+-----WAN2------+--EN--+--------LEDS---------
    LNK RDY CH1 Ch2   LNK  LNK    LNK RDY CH1 CH2  DATA │ '-'= Off 'G'= Green
 G   -   -   -   -     -    -      -   -   -   -    Y   │ 'R'= Red 'Y'= Yellow

```

Current Date: The current date; this can be set with the Date and Time utility (see "Date and Time" on page 8-14).

Default IP Gateway: The router's default gateway, which may be either manually configured or learned via DHCP. This is the value you assigned in the Default IP Gateway field on page 7-10. If you are using the router's defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

CPU Load: Percentage of the system's resources being used by all current transmissions.

Unused Memory: The total remaining system memory available for use.

Domain Name Server: If you are using the router's defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

Call Acct: Shows whether you have enabled or disabled the call accounting features.

Domain Name: the domain name you have assigned, typically the name of your ISP

MAC Address: The Netopia R3100's hardware address, for those interfaces that support DHCP.

IP Address: The Netopia R3100's IP address, entered in the IP Setup screen.

IPX Address: The Netopia R3100's IPX address, entered in the IPX Setup screen.

EtherTalk Address: The Netopia R3100's AppleTalk address on its EtherTalk Phase II interface, entered in the EtherTalk Phase II Setup screen (only if the optional AppleTalk feature set is installed).

LocalTalk Address: The Netopia R3100's AppleTalk address on its LocalTalk interface, entered in the LocalTalk Setup screen (only if the optional AppleTalk feature set is installed).

Current status

The current status section is a table showing the current status of the WAN. For example:

```
                         Current WAN Connection Status
        ---Profile Name------State---%Use-Remote Address----Est.-More Info----------
        ISP                  P1      10  IP 92.163.4.1      Lcl  NAT 192.163.100.6
```

Profile Name: Lists the name of the connection profile being used, if any.

State: Lists the ports in use for this connection.

%Use: Indicates the average percent utilization of the maximum capacity of the channels in use for the connection.

Remote Address: Shows the IP address of the connected remote router if the connection is using IP. Otherwise, shows the IPX address of the connected remote router, if using IPX.

Est: Indicates whether the connection was locally ("Lcl") or remotely ("Rmt") established.

More Info: Indicates, in order of priority, the NAT address in use for this connection, the IPX address in use (if IP is also in use), or the ISDN caller identification (if available).

Status lights

This section shows the current real-time status of the Netopia R3100's status lights (LEDs). It is useful for remotely monitoring the router's status. The Quick View screen's arrangement of LEDs corresponds to the physical arrangement of LEDs on the router.

```
-PWR-+-----WAN1------+--CON--AUX--+-----WAN2------+--EN--+--------LEDS---------
      LNK RDY CH1 Ch2    LNK  LNK    LNK RDY CH1 CH2  DATA | '-'= Off 'G'= Green
  G    -   G   -   -     Y    -      -   -   -   -     -   | 'R'= Red 'Y'= Yellow
```

Each LED representation can report one of four states:

–: A dash means the LED is off.

R: The letter "R" means the LED is red.

G: The letter "G" means the LED is green.

Y: The letter "Y" means the LED is yellow.

The section "Netopia R3100 ISDN Router Status Lights" on page 2-6 describes the meanings of the colors for each LED.

Statistics & Logs

```
┌──────────┐          ┌──────────────────┐          ┌─────────────────────┐
│   Main   │   ───▶   │ Statistics & Logs│   ───▶   │ • General Statistics│
│   Menu   │          │                  │          │                     │
└──────────┘          └──────────────────┘          └─────────────────────┘
```

When you are troubleshooting your Netopia R3100, the Statistics & Logs screens provide insight into the recent event activities of the router.

From the Main Menu go to **Statistics & Logs** and select one of the options described in the sections below.

General Statistics

To go to the General Statistics screen, select **General Statistics** and press Return. The General Statistics screen appears.

```
                        General Statistics

Phys I/F---------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
Ethernet Hub    123456789  123456789  12345678  12345678  12345678  12345678
LocalTalk       123456789  123456789
ISDN B1 Chan    123456789  123456789  12345678  12345678
ISDN B2 Chan    123456789  123456789  12345678  12345678
ISDN D Chan     123456789  123456789  12345678  12345678


Network----------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
IP              123456789  123456789  12345678  12345678  12345678  12345678
IPX             123456789  123456789  12345678  12345678  12345678  12345678
AppleTalk       123456789  123456789  12345678  12345678
```

The General Statistics screen displays information about data traffic on the Netopia R3100's data ports. This information is useful for monitoring and troubleshooting your LAN. Note that the counters roll over at their maximum field width, that is, they restart again at 0.

Physical Interface

The top left side of the screen lists total packets received and total packets transmitted for the following data ports:

■ Ethernet Hub

■ Aux Async or LocalTalk (if the optional AppleTalk feature set is installed)

■ ISDN B1 Channel

■ ISDN B2 Channel

■ ISDN D Channel

Network Interface

The bottom left side of the screen lists total packets received and total packets transmitted for the following protocols:

■ IP (IP packets on the Ethernet)

■ IPX (IPX packets on the Ethernet) if IPX is enabled

■ AppleTalk (AppleTalk packets on Ethernet using EtherTalk Phase II if the optional AppleTalk feature set is installed)

■ LT (LocalTalk on the PhoneNET) if the optional AppleTalk feature set is installed

The right side of the table lists the total number of occurrences of each of six types of communication statistics:

Rx Bytes. The number of bytes received

Tx Bytes. The number of bytes transmitted

Rx Packets: The number of packets received

Tx Pkts. The number of packets transmitted

Rx Err: The number of bad Ethernet packets received

Tx Err: An error occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN

Event histories

The Netopia R3100 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R3100's built-in battery backup prevents loss of event history from a shutdown or reset.

The router's event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History retain records of the 128 most recent events.

In the Statistics & Logs screen, select **WAN Event History**. The WAN Event History screen appears.

```
   ┌──────────┐         ┌─────────────────┐         ┌───────────────────────┐
   │  Main    │────────▶│ Statistics & Logs│────────▶│ • WAN Event History   │
   │  Menu    │         │                 │         │ • Device Event History │
   └──────────┘         └─────────────────┘         └───────────────────────┘
```

WAN Event History

The WAN Event History screen lists a total of 128 events on the WAN. The most recent events appear at the top.

```
                            WAN Event History
                                      Current Date --   9/4/98 01:09:49 PM
       -Date-----Time-----Event------------------------------------------------
       -------------------------------SCROLL UP---------------------------------
       09/04/98 12:58:34   Link 1 down: Remote clearing, cause: 41, diag: 22
       09/04/98 12:58:34   Issued Clear Response to DN: 5105776430
       09/04/98 12:58:34   Received Clear Ind. from DN: 5105776430, Cause: 41
       09/04/98 12:58:32   Requested Disc. from DN: 5105776431
       09/04/98 12:58:24 >>Issued 64Kb Setup Request from our DN: 5105776430
       09/04/98 10:35:54   Link 2 down: Remote clearing, cause: 41, diag: 50
       09/04/98 10:35:54   Issued Clear Response to DN: 5105776431
       09/04/98 10:35:54   Received Clear Ind. from DN: 5105776431, Cause: 41
       09/04/98 10:35:54   Link 1 down: Remote clearing, cause: 41, diag: 50
       09/04/98 10:35:54   Issued Clear Response to DN: 5105776430
       09/04/98 10:35:54   Received Clear Ind. from DN: 5105776430, Cause: 41
       09/04/98 10:35:44 >>Issued Speech Setup Request from our DN: 5105776431
       09/04/98 10:35:44 >>Issued Speech Setup Request from our DN: 5105776430
       09/04/98 10:35:44 --Device restarted--------------------------------------
       ------------------------------SCROLL DOWN--------------------------------
       Clear History...


      Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

Each entry in the list contains the following information:

Time: Time of the event.

Date: Date of the event.

Event: A brief description of the event.

Ch.: The channel involved in the event.

Dir. Number: The directory number (number dialed) involved in the event (switched circuit models only).

The first event in each call sequence is marked with double arrows (>>).

Failures are marked with an asterisk (*).

If the event history exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To get more information about any event listed in the WAN Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or Escape to dismiss the dialog box.

To clear the event history, select **Clear History** at the bottom of the history screen and press Return.

For more information on Event Cause Codes see Appendix H, "Event Histories."

Device Event History

The Device Event History screen lists a total of 128 port and system events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

In the Statistics & Logs screen, select **Device Event History**. The Device Event History screen appears.

```
                        Device Event History
                             Current Date --   9/4/98 01:10:19 PM
    -Date-----Time-----Event-------------------------------------------------
    -------------------------------SCROLL UP----------------------------------
    09/04/98 13:09:28   Telnet connection up, address 192.168.1.100
    09/04/98 12:58:50   Telnet connection down, address 192.168.1.100
    09/04/98 12:57:04   Telnet connection up, address 192.168.1.100
    09/04/98 10:39:28   Telnet connection up, address 192.168.1.104
    09/04/98 10:35:51   AppleTalk initialization complete
    09/04/98 10:35:44   IP address server initialization complete
    09/04/98 10:35:44 --BOOT: Warm start v4.2a2 --------------------------------
    09/04/98 09:17:59   Telnet connection up, address 192.168.1.104
    09/04/98 09:09:07   AppleTalk initialization complete
    09/04/98 09:09:00   IP address server initialization complete
    09/04/98 09:09:00 --BOOT: Cold start v4.2a2 --------------------------------
    09/03/98 17:22:24   Telnet connection down, address 192.168.1.104
    09/03/98 13:54:20   Telnet connection down, address 192.168.1.100
    09/03/98 13:50:41   Telnet connection up, address 192.168.1.100
    ------------------------------SCROLL DOWN---------------------------------
    Clear History...


     Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

If the event history exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To obtain more information about any event listed in the Device Event History, select the event and then press Return. A dialog box containing more information about the selected event appears. Press Return or Escape to dismiss the dialog box.

To clear the Device Event History, select **Clear History** and press Return.

Routing tables

You can view all of the IP, IPX, and AppleTalk routes in the Netopia R3100's IP, IPX, and AppleTalk routing tables, respectively.

To go to a routing table screen, select the routing table you are interested in from the **Statistics & Logs** screen.

Each of the routing table screens represents a "snapshot" of the routing table information at the time the screen is first invoked. To take a new snapshot, select **Update** at the bottom of the screen and press Return.

```
                            Statistics & Logs

                    WAN Event History...
                    Device Event History...

                    IP Routing Table...

                    IPX Routing Table...
                    IPX SAP Bindery Table...

                    AppleTalk Routing Table...

                    Served IP Addresses...

                    General Statistics...

                    System Information...
```
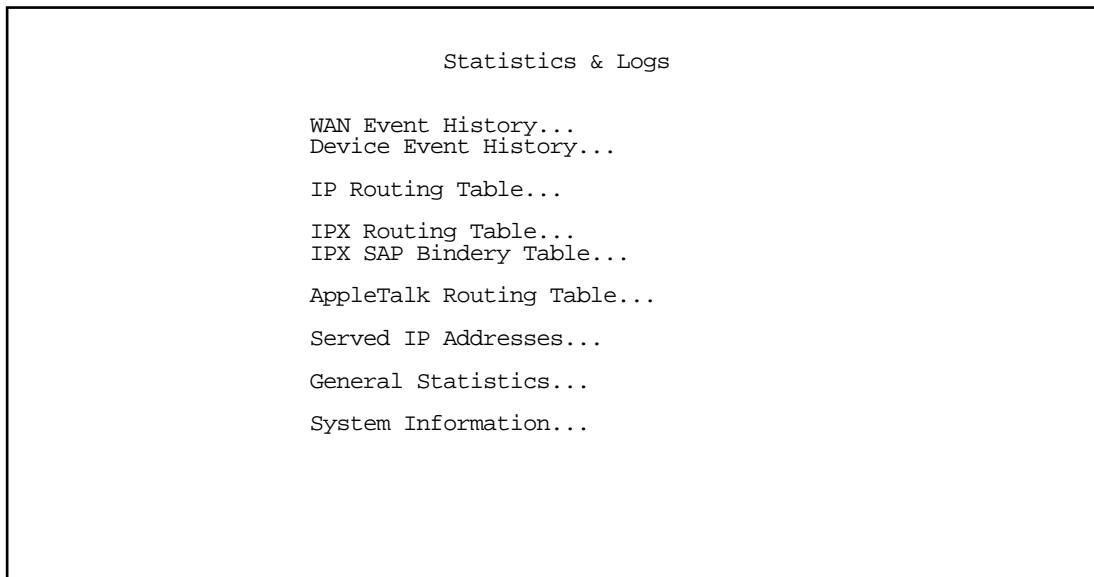
IP routing table

In the Statistics & Logs screen, select **IP Routing Table** and press Return.

The IP routing table displays all of the IP routes currently known to the Netopia R3100.

```
                            IP Routing Table

 Network Address-Subnet Mask-----via Router------Port-----------------Type----
 --------------------------------SCROLL UP-------------------------------------
 0.0.0.0          255.0.0.0       0.0.0.0          --                    Other
 127.0.0.1        255.255.255.255 127.0.0.1        Loopback             Local
 192.168.1.0      255.255.255.240 192.168.1.1      Ethernet             Local
 192.168.1.1      255.255.255.255 192.168.1.1      Ethernet             Local
 192.168.1.15     255.255.255.255 192.168.1.15     Ethernet             Bcast
 224.0.0.0        224.0.0.0       0.0.0.0          --                    Other
 255.255.255.255 255.255.255.255 255.255.255.255 --                     Bcast




 --------------------------------SCROLL DOWN-----------------------------------
 UPDATE
```

IPX routing table

In the Statistics & Logs screen, select **IPX Routing Table** and press Return.

The IPX routing table displays all of the IPX routes currently known to the Netopia R3100.

IPX Sap Bindery table

In the Statistics & Logs screen, select **IPX Sap Bindery Table** and press Return.

The IPX Sap Bindery table displays all of the IPX Sap Bindery routes currently known to the Netopia R3100.

AppleTalk routing table

In the Statistics & Logs screen, select **AppleTalk Routing Table** and press Return. An AT Routing Table similar to the one shown below will appear.

The AppleTalk routing table displays information about the current state of AppleTalk networks connected to the Netopia R3100, including remote AppleTalk networks connected with AURP. This information is gathered from other active AppleTalk routers.

```
                      AT Routing Table

 -Net---Range--Def Zone Name----------Hops-State-Next Rtr Addr.--Pkts Fwded
   ------------------------------SCROLL UP------------------------
    1      --     Admin                2     Good  46.131           0
    2      --     AdMan                2     Good  46.131           0
    3      --     Aspirations          2     Good  46.131           0
    4      --     Sales                2     Good  46.131           0
    5      --     Marketing            2     Good  46.131           0
    6      --     Molluscs             2     Good  46.131           1
    7      --     Customer Service     2     Good  46.131           1
    8      --     Telemarketing        2     Good  46.131           0
   10      --     Rio                  2     Good  46.131           0
   11      --     Regiment             2     Good  46.131           0
   12      --     Rhinos               2     Good  46.131           0
   16      --     Unique Services      2     Good  46.131           0
  *24      27     Aspirations          1     Good  46.131          79
   28      31     Rhinos               1     Good  46.131          15
   -----------------------------SCROLL DOWN-----------------------
 UPDATE

 '*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

Each row in the AppleTalk routing table corresponds to an AppleTalk route or network range. If the list of routes shown exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the table and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the table and press Return.

The table has the following columns:

Net: Displays the starting network number supplied by the AppleTalk router in the "Next Rtr Addr." column. If a network number is preceded by an asterisk (*), it has multiple zones. To display the zones, select the network entry and press Return.

Range: Displays the ending network number for the extended network.

Def Zone Name: Displays the zone or zones associated with the specified network or network range. The zone name shown is either the only zone or the default zone name for an extended network. To see the complete list of zones for an extended network with multiple zones, select the entry in the table and press Return. Press Return again to close the list of zones.

Hops: Displays the number of routers between the Netopia R3100 and the specified network.

State: Displays the state of the specified route, based on the frequency of Routing Table Maintenance Protocol (RTMP) packets received for the route. The state can be Good, Suspect, or Bad. AppleTalk routers regularly exchange RTMP packets to update AppleTalk routing information.

Next Rtr Addr.: Displays the DDP or IP address of the next hop for the specified route. A DDP address is displayed if the router shown is on the local AppleTalk network. DDP address means that a connection to the next-hop router is by a native AppleTalk network (e.g.: LocalTalk or EtherTalk Phase II). An IP address is displayed if the Netopia R3100 is connected to the router shown using AURP. IP address means a connection transports over AURP (AppleTalk encapsulated IP).

Pkts Fwded: The number of packets sent to the router shown.

Served IP Addresses

You can view all of the IP addresses currently being served by the Netopia R3100 ISDN Router from the **Served IP Addresses** screen.

From the Statistics & Logs menu, select **Served IP Addresses**. The Served IP Addresses screen appears.

```
                          Served IP Addresses

    -IP Address-------Type----Expires--Client Identifier------------------------
    ------------------------------------SCROLL UP---------------------------------
     192.168.1.100    DHCP     00:36     EN: 00-00-c5-4a-1f-ea
     192.168.1.101    DHCP     00:58     EN: 08-00-07-16-0c-85
     192.168.1.102
     192.168.1.103
     192.168.1.104
     192.168.1.105
     192.168.1.106
     192.168.1.107
     192.168.1.108
     192.168.1.109
     192.168.1.110
     192.168.1.111
     192.168.1.112
     192.168.1.113
    --------------------------------SCROLL DOWN-----------------------------------
    Lease Management...


       EN = Ethernet Address; AT = AppleTalk Address; CP = Profile Name; HX = hex
```

To manage DHCP leases, select **Lease Management** in this screen.

The IP Address Lease Management screen appears.

```
                        IP Address Lease Management

                Reset All Leases...

                Release BootP Leases...

                Reclaim Declined Addresses...
```

This screen has three options:

- **Reset All Leases**: Resets all current IP addresses leased through DHCP without waiting for the default one–hour lease period to elapse

- **Release BootP Leases**: Releases any BootP leases that may be in place, and which may no longer be required.

- **Reclaim Declined Addresses**: Reclaims served leases that have been declined; for example by devices that may no longer be on the network.

System Information

The System Information screen gives a summary view of the general system level values in the Netopia R3100 ISDN Router.

From the Statistics & Logs menu select **System Information**. The System Information screen appears.

```
                    System Information


      Serial Number                 07-30-44 (8680437)
      Firmware Version              4.2


      Processor Speed (MHz)         33
      Flash ROM Capacity (MBytes)   1
      DRAM Capacity (MBytes)        4

      Ethernet                      8 Port 10Base-T
      Auxiliary Serial Port         Switched Async
      WAN 1 Interface               ISDN ST-POTS
      WAN 2 Interface               Not Installed

      AppleTalk Feature Set         Not Installed
```

The information display varies by model, firmware version, feature set, and so on. You can tell at a glance your particular system configuration.

SNMP

The Netopia R3100 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

The Netopia R3100 supports the following management information base (MIB) documents:

■　MIB II (RFC 1213)

■　Interface MIB (RFC 1229)

■　Ethernet MIB (RFC 1643)

■　AppleTalk MIB I (RFC 1243)

■　Netopia MIB

These MIBs are on the Netopia R3100 CD included with the Netopia R3100. Load these MIBs into your SNMP management software in the order they are listed here. Follow the instructions included with your SNMP manager on how to load MIBs.

The SNMP Setup screen

From the Main Menu, select **SNMP** in the System Configuration screen and press Return. The SNMP Setup screen appears.

```
┌──────────────┐      ┌──────────────┐      ┌──────────────┐
│    Main      │─────▶│    System    │─────▶│    SNMP      │
│    Menu      │      │ Configuration│      │              │
└──────────────┘      └──────────────┘      └──────────────┘
```

```
                           SNMP Setup


          System Name:
          System Location:
          System Contact:


          Read-Only Community String:              public
          Read/Write Community String:             private

          Authentication Traps Enable:             Off

          IP Trap Receivers...




  Configure optional SNMP parameters from here.

```
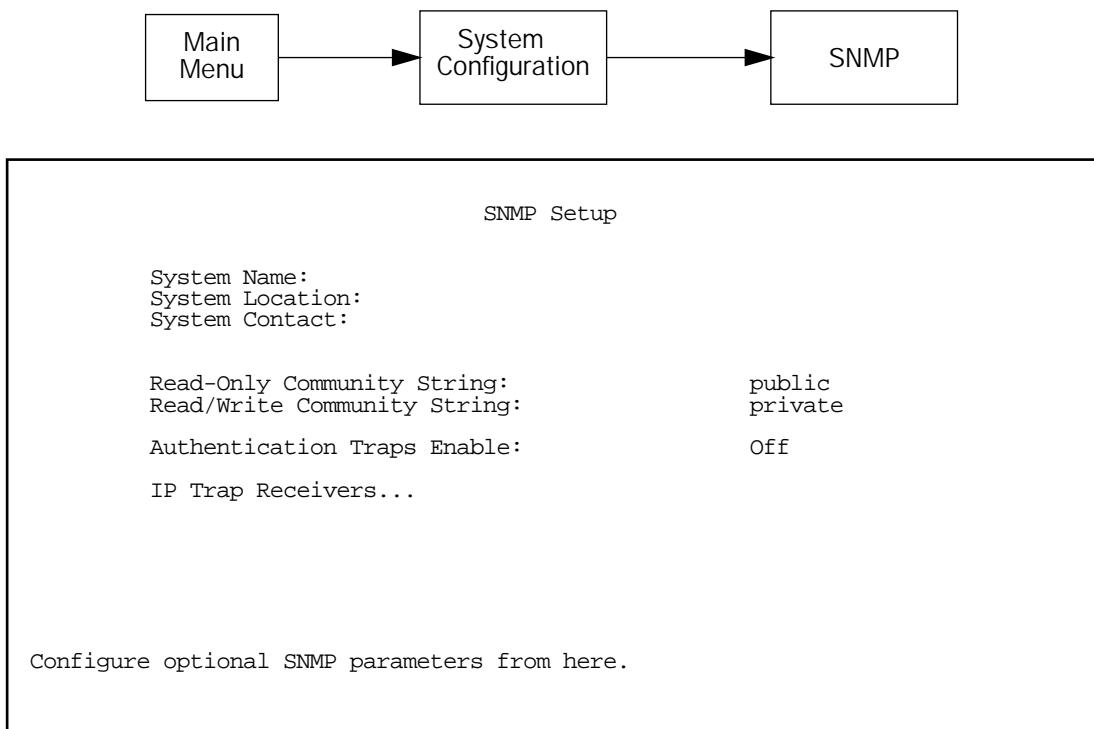
Follow these steps to configure the first three items in the screen:

1. Select **System Name** and enter a descriptive name for the Netopia R3100's SNMP agent.

2. Select **System Location** and enter the router's physical location (room, floor, building, etc.).

3. Select **System Contact** and enter the name of the person responsible for maintaining the router.

System Name, System Location, and System Contact set the values returned by the Netopia R3100 SNMP agent for the SysName, SysLocation, and SysContact objects, respectively, in the MIB II system group. Although optional, the information you enter in these items can help a system administrator manage the network more efficiently.

Community strings

The **Read-Only Community String** and the **Read/Write Community String** are like passwords that must be used by an SNMP manager querying or configuring the Netopia R3100. An SNMP manager using the **Read-Only Community String** can examine statistics and configuration information from the router, but cannot modify the router's configuration. An SNMP manager using the **Read/Write Community String** can both examine and modify configuration parameters.

By default, the read-only and read/write community strings are set to "public" and "private," respectively. You should change both of the default community strings to values known only to you and trusted system administrators.

To change a community string, select it and enter a new value.

Caution! Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Netopia R3100 through SNMP. For more information on security issues, see "Suggested security measures" on page 15-1.

SNMP traps

An SNMP **trap** is an informational message sent from an SNMP agent (in this case, the Netopia R3100) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

Standard traps generated by the Netopia R3100 include the following:

■ An authentication failure trap is generated when the router detects an incorrect community string in a received SNMP packet. **Authentication Traps Enable** must be **On** for this trap to be generated.

■ A cold start trap is generated after the router is reset.

■ An interface down trap (ifDown) is generated when one of the router's interfaces, such as a port, stops functioning or is disabled.

■ An interface up trap (ifUp) is generated when one of the router's interfaces, such as a port, begins functioning.

The Netopia R3100 sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia R3100. Up to eight receivers can be set. You can also review and remove IP traps.

To go to the IP Trap Receivers screen, select **IP Trap Receivers**. The IP Trap Receivers screen appears.

```
                          IP Trap Receivers


                Display/Change IP Trap Receiver...

                Add IP Trap Receiver...

                Delete IP Trap Receiver...


   Return/Enter to modify an existing Trap Receiver.
   Navigate from here to view, add, modify and delete IP Trap Receivers.
```
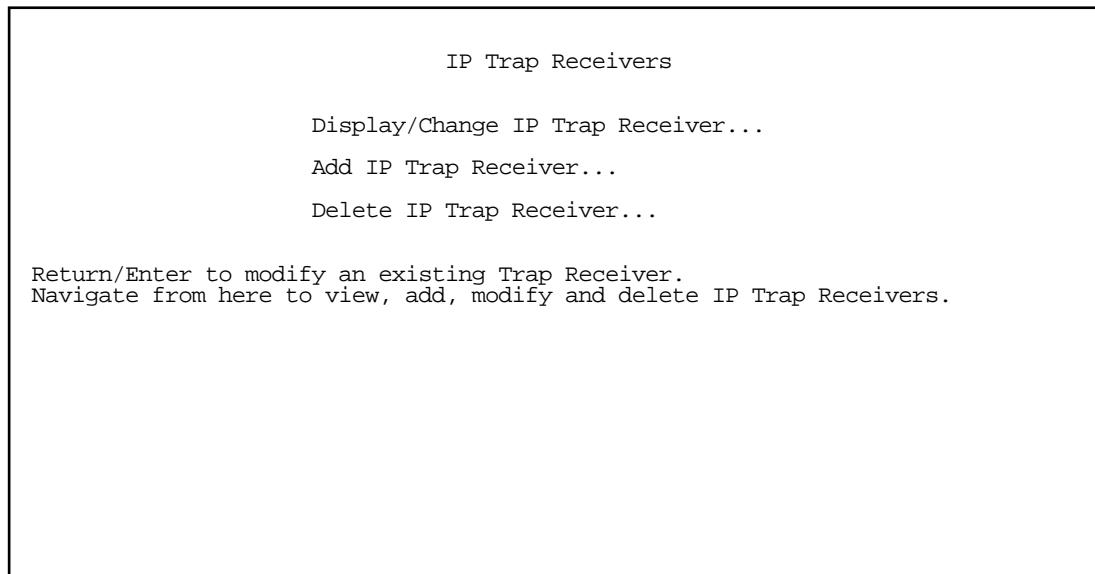
Setting the IP trap receivers

1.   Select **Add IP Trap Receiver**.

2.   Select **Receiver IP Address or Domain Name**. Enter the IP address or domain name of the SNMP manager you want to receive the trap.

3.   Select **Community String**. Enter whatever community string is appropriate for the traps to be sent to the management station whose IP address or domain name you entered on the previous line.

4.   Select **Add Trap Receiver Now** and press Return. You can add up to seven more receivers.

Viewing IP trap receivers

To display a view-only table of IP trap receivers, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.

Modifying IP trap receivers

1.   To edit an IP trap receiver, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.

2.   Select an IP trap receiver from the table and press Return.

3.   In the **Change IP Trap Receiver** screen, edit the information as needed and press Return.

Deleting IP trap receivers

1.   To delete an IP trap receiver, select **Delete IP Trap Receiver** in the IP Trap Receivers screen.

2.   Select an IP trap receiver from the table and press Return.

3.   In the dialog box, select **Continue** and press Return.

Chapter 15

Security

The Netopia R3100 provides a number of security features to help protect its configuration screens and your local network from unauthorized access. Although these features are optional, it is strongly recommended that you use them.

This section covers the following topics:

Suggested security measures

In addition to setting up user accounts, Telnet access, and filters (all of which are covered later in this chapter), there are other actions you can take to make the Netopia R3100 and your network more secure:

■   Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.

■   Set the answer profile so it must match incoming calls to a connection profile.

■   Use CallerID.

■   Leave the "Enable Dial-in Console Access" option set to No.

■   Where possible, insist on using PAP, CHAP, or secure authentication token card to authenticate connections to and from connection profiles.

■   When using AURP, accept connections only from configured partners.

■   In high risk areas, configure the Netopia R3100 through the serial console port to ensure that your communications cannot be intercepted.

User accounts

When you first set up and configure the Netopia R3100, no passwords are required to access the configuration screens. Anyone could tamper with the router's configuration by simply connecting it to a console.

However, by adding user accounts, you can protect the most sensitive screens from unauthorized access. User accounts are composed of name/password combinations that can be given to authorized users.

Caution!

You are strongly encouraged to add protection to the configuration screens. Unprotected screens could allow an unauthorized user to compromise the operation of your entire network.

Once user accounts are created, users who attempt to access protected screens will be challenged. Users who enter an incorrect name or password are returned to a screen requesting a name/password combination to access the Main Menu.

To set up user accounts, select **Security** in the System Configuration screen and go to the Security Options screen.

```
                           Security Options

        Enable Dial-in Console Access:                    Yes

        Enable SmartStart/SmartView/Web Server:           Yes

        Enable Telnet Console Access:                     Yes
        Enable Telnet Access to SNMP Screens:             Yes


        Show Users...
        Add User...
        Delete User...


        Password for This Screen (11 chars max):



 Return/Enter accepts * Tab toggles * ESC cancels.
 Set up configuration access options here.
```

Protecting the Security Options screen

The first screen you should protect is the Security Options screen, because it controls access to the configuration screens. Access to the Security Options screen can be protected with a password.

Select **Password for This Screen** in the Security Options screen and enter a password. Make sure this password is secure and is different from any of the user account passwords.

Protecting the configuration screens

You can protect the configuration screens with user accounts. You can administer the accounts from the Security Options screen. You can create up to four accounts.

To display a view-only list of user accounts, select **Show Users** in the Security Options screen.

To add a new user account, select **Add User** in the Security Options screen and press Return to go to the Add Name With Write Access screen.

```
                      Add Name With Write Access

        Enter Name:
        Enter Password (11 characters max):




        ADD NAME/PASSWORD NOW               CANCEL
```
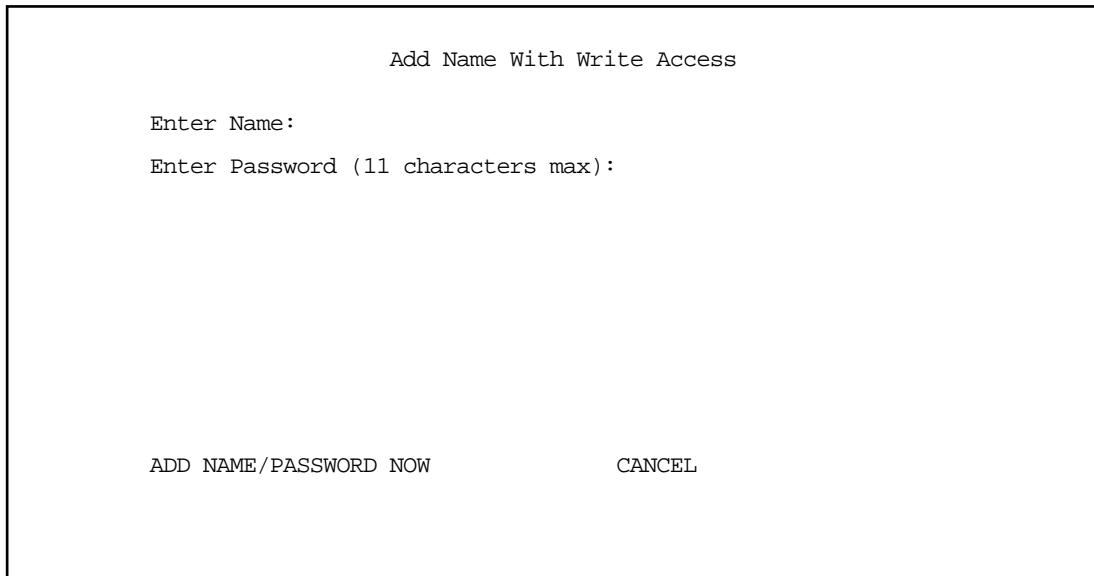
Follow these steps to configure the new account:

1. Select **Enter Name** and enter a descriptive name (for example, the user's first name).

2. Select **Enter Password** and enter a password.

3. To accept the new name/password combination, select **ADD NAME/PASSWORD NOW**. To exit the Add Name With Write Access screen without saving the new account, select **CANCEL**.

To delete a user account, select **Delete User** to display a list of accounts. Select an account from the list and press Return to delete it. To exit the list without deleting the selected account, press the Escape key.

Dial-in Console Access

Remote modem terminal emulator setups can dial in to either internal modem line and establish a remote console session, even though they are not using PPP. This allows Netopia Inc.'s "Up and Running, Guaranteed!" department or other administrator with the appropriate security to remotely configure your router for you. If you used SmartStart to configure your router, this option will be set to "No".

■   To prevent any remote caller from establishing a remote session, change the option **Enable Dial-in Console Access** to "No".

■   To allow access for Up and Running, Guaranteed! with the default name and password in place, toggle this option to "Yes".

Enable SmartStart/SmartView/Web Server

You may wish to restrict access to the web-based screens to prevent inadvertent switching or connecting and disconnecting of Connection Profiles. Since SmartStart can be used to reconfigure the router, you may wish to block inadvertent damage resulting from unauthorized use of SmartStart. To prevent access to these features toggle this option to "No".

Telnet access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. The Netopia R3100 supports Telnet access to its configuration screens.

Caution!

You should consider password-protecting or restricting Telnet access to the Netopia R3100 if you suspect there is a chance of tampering.

To password-protect the configuration screens, select Easy Setup from the Main Menu, and go to the **Easy Setup Security Configuration** screen. By entering a Name and Password pair in this screen, all access via serial, Telnet, SNMP, and web server will be password-protected.

To restrict Telnet access, select **Security** in the Advanced Configuration Menu and go to the Security Options screen. There are two levels of Telnet restriction available:

To restrict Telnet access to the SNMP screens, select **Enable Telnet Access to SNMP Screens** and toggle it to **No**. (See "SNMP traps" on page 14-14.)

To restrict Telnet access to all of the configuration screens, select **Enable Telnet Console Access** and toggle it to **No**.

About filters and filter sets

Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network's security.

The Netopia R3100's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the router's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called firewalling your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What's a filter and what's a filter set?

A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can either be an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to see if it matches that destination.

A filter inspects data packets like a customs inspector scrutinizing packages.

Filter priority

Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.

packet

first
filter

match?

no
send
to next
filter

yes

pass or
discard?

discard
(delete)

pass

to network
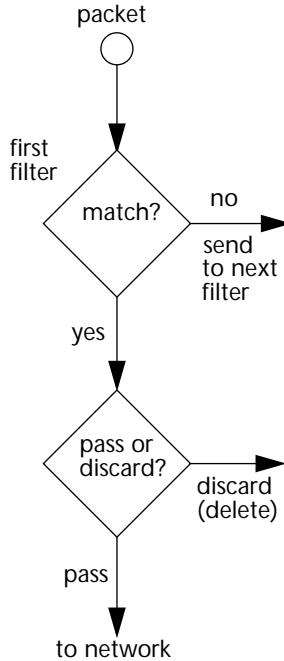
If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, and so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can pass or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither pass nor discard the packet (because it cannot match any criteria), the second filter has a chance to pass or reject it, and so on. Because of this hierarchical structure, each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

A filter's actions

■ Passes the packet to the local or remote network

■ Blocks (discards) the packet

■ Ignores the packet

A filter passes or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

A filtering rule

Block all Telnet attempts that originate from the remote host 199.211.211.17.

This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.

Here is what this rule looks like when implemented as a filter on the Netopia R3100:

```
+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------+
| 1  199.211.211.17  0.0.0.0          TCP   23              Yes No  |
+-------------------------------------------------------------------+
```

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

■ The source IP address (where the packet was sent from)

■ The destination IP address (where the packet is going)

■ The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Port numbers

A filter can also match a packet's port number attributes, but only if the filter's protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

■   The source port number (the port on the sending host that originated the packet)

■   The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The tables below show a few common services and their associated port numbers..

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80
SMTP (mail)	25	News	144
Gopher	70	rlogin	513

Internet service	UDP port	Internet service	UDP port
Who Is	43	AppleTalk Routing Maintenance (at-rtmp)	202
World Wide Web	80	AppleTalk Name Binding (at-nbp)	202
SNMP	161	AURP (AppleTalk)	387
TFTP	69	who	513

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

No Compare: No comparison of the port number specified in the filter with the packet's port number.

Not Equal To: For the filter to match, the packet's port number cannot equal the port number specified in the filter.

Less Than: For the filter to match, the packet's port number must be less than the port number specified in the filter.

Less Than or Equal: For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.

Equal: For the filter to match, the packet's port number must equal the port number specified in the filter.

Greater Than: For the filter to match, the packet's port number must be greater than the port number specified in the filter.

Greater Than or Equal: For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

Other filter attributes

There are three other attributes to each filter:

■   The filter's order (i.e., priority) in the filter set

■   Whether the filter is currently active

■   Whether the filter is set to pass (forward) packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+---------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0             TCP    0         23      Yes No  |
| 2   0.0.0.0          0.0.0.0             TCP    NC        =6000   Yes No  |
| 3   0.0.0.0          0.0.0.0             ICMP   --        --      Yes Yes |
| 4   0.0.0.0          0.0.0.0             TCP    NC        >1023   Yes Yes |
| 5   0.0.0.0          0.0.0.0             UDP    NC        >1023   Yes Yes |
|                                                                     |
|                                                                     |
|                                                                     |
|                                                                     |
|                                                                     |
+---------------------------------------------------------------------+
```

The table's columns correspond to each filter's attributes:

#: The filter's priority in the set. Filter number 1, with the highest priority, is first in the table.

Source IP Addr: The packet source IP address to match.

Dest IP Addr: The packet destination IP address to match.

Proto: The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if using those protocols.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol

Protocol	Number to use	Full name
UDP	17	User Datagram Protocol

Src. Port: The source port to match. This is the port on the sending host that originated the packet.

D. Port: The destination port to match. This is the port on the receiving host for which the packet is intended.

On?: Displays **Yes** when the filter is in effect or **No** when it is not.

Fwd: Shows whether the filter forwards (**Yes**) a packet or discards (**No**) it when there's a match.

Filtering example #1

Returning to our filtering rule example from above (see page 15-7), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

1. The rule you want to implement as a filter is:

   Block all Telnet attempts that originate from the remote host 199.211.211.17.

2. The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Dest IP Addr could have been anything. The mask for Source IP Addr must be 255.255.255.255 since an exact match is desired.

   ■ Source IP Addr = 199.211.211.17

   ■ Source IP address mask = 255.255.255.255

   ■ Dest IP Addr = 0.0.0.0

   ■ Destination IP address mask = 0.0.0.0

   Note: To learn about IP addresses and masks, see Appendix E, "Understanding IP Addressing."

3. Using the tables on page 15-8, find the destination port and protocol numbers (the *local* Telnet port):

   ■ Proto = TCP (or 6)

   ■ D. Port = 23

4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:

   ■ On? = Yes

   ■ Fwd = No

This four-step process is how we produced the following filter from the original rule:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+---------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0            TCP   0        23      Yes No |
|                                                                     |
+---------------------------------------------------------------------+
```

Filtering example #2

Suppose a filter is configured to block all incoming IP packets with the source IP address of 200.233.14.0, regardless of the type of connection or its destination. The filter would look like this:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+---------------------------------------------------------------------+
| 1   200.233.14.0     0.0.0.0                   0               Yes No |
|                                                                     |
+---------------------------------------------------------------------+
```

This filter blocks any packets coming from a remote network with the IP network address 200.233.14.0. The 0 at the end of the address signifies *any* host on the class C IP network 200.233.14.0. If, for example, the filter is applied to a packet with the source IP address 200.233.14.5, it will block it.

In this case, the mask, which does not appear in the table, must be set to 255.255.255.0. This way, all packets with a source address of 200.233.14.x will be matched correctly, no matter what the final address byte is.

Note: The protocol attribute for this filter is 0 by default. This tells the filter to ignore the IP protocol or type of IP packet.

Design guidelines

Careful thought should go into designing a new filter set. You should consider the following guidelines:

■ Be sure the filter set's overall purpose is clear from the beginning. A vague purpose can lead to a faulty set, and that can actually make your network *less* secure.

■ Be sure each individual filter's purpose is clear.

■ Determine how filter priority will affect the set's actions. Test the set (on paper) by determining how the filters would respond to a number of different hypothetical packets.

■ Consider the combined effect of the filters. If every filter in a set fails to match on a particular packet, the packet is:

    ■ passed if all the filters are configured to discard (*not* forward).

    ■ discarded if all the filters are configured to pass (forward).

    ■ discarded if the set contains a combination of pass and discard filters.

Disadvantages of filters

Although using filter sets can greatly enhance network security, there are disadvantages:

■   Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.

■   Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints.

■   Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, caller ID, the "must match" option in the answer profile, PAP or CHAP in connection profiles, callback, and general awareness of how your network may be vulnerable.

An approach to using filters

The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

Each filter set you design will be based on one of the following approaches:

■   That which is not expressly prohibited is permitted.

■   That which is not expressly permitted is prohibited.

It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.

Working with IP filters and filter sets

This section covers IP filters and filter sets. For working with IPX filters and filter sets, see "IPX filters" on page 15-22.

```
┌──────────┐      ┌────────────────┐      ┌────────┐      ┌────────────────┐
│   Main   │ ───▶ │     System     │ ───▶ │ Filter │ ───▶ │  IP Filter Sets │
│   Menu   │      │ Configuration  │      │  Sets  │      │                │
└──────────┘      └────────────────┘      └────────┘      └────────────────┘
```
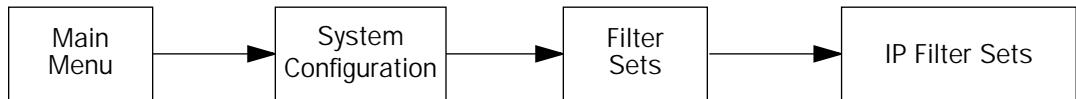
To work with filters and filter sets, begin by accessing the filter set screens.

Note: Make sure you understand how filters work before attempting to use them. Read the section "About filters and filter sets," beginning on page 15-4.

```
                          IP Filter Sets

                  Display/Change IP Filter Set...

                  Add IP Filter Set...

                  Delete IP Filter Set...








    Return/Enter to configure and add a new Filter Set
    Set Up IP Filter Sets (Firewalls) from this and the following Menus.
```

The procedure for creating and maintaining filter sets is as follows:

1.   Add a new filter set.

2.   Create the filters for the new filter set.

3.   View, change, or delete individual filters and filter sets.

The sections below explain how to execute these steps.

Adding a filter set

You can create up to eight different custom filter sets. Each filter set can contain up to 16 output filters and up to 16 input filters.

To add a new filter set, select **Add IP Filter Set** in the IP Filter Sets screen and press Return to go to the Add Filter Set screen.

Note: There are two groups of items in the Add Filter Set screen, one for input filters and one for output filters. The two groups work in essentially the same way, as you'll see below.

```
                              Add IP Filter Set

           Filter Set Name:                    Filter Set  2

           Display/Change Input Filter...
           Add Input Filter...
           Delete Input Filter...

           Display/Change Output Filter...
           Add Output Filter...
           Delete Output Filter...




           ADD FILTER SET                       CANCEL

    Configure the Filter Set name and its associated Filters.
```
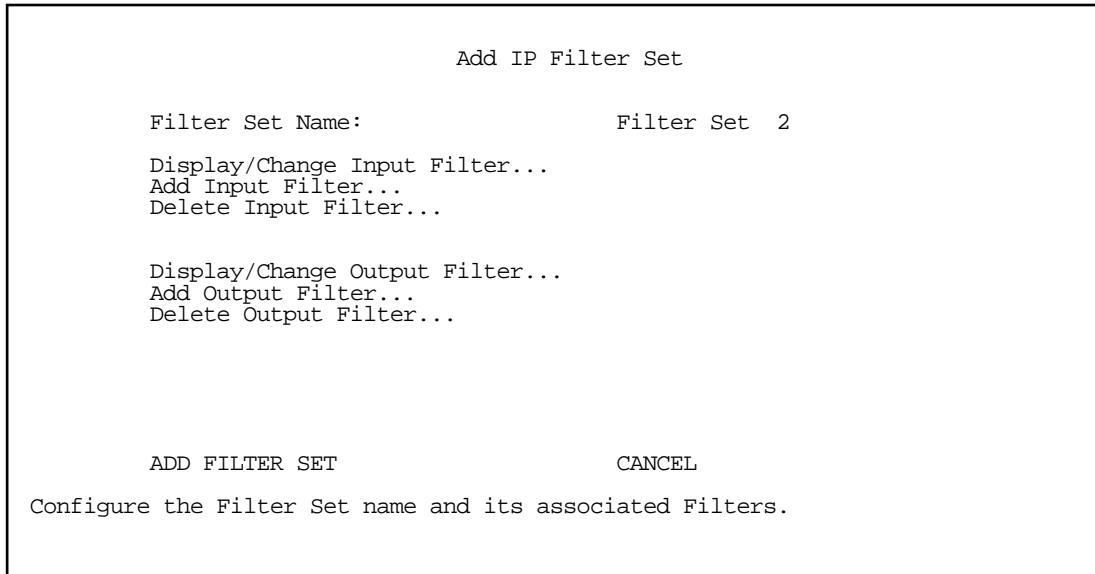
Naming a new filter set

All new filter sets have a default name. The first filter set you add will be called Filter Set 1, the next filter will be Filter Set 2, and so on.

To give a new filter set a different name, select **Filter Set Name** and enter a new name for the filter set.

To save the filter set, select **ADD FILTER SET**. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see "Modifying filter sets" on page 15-18). Or you can add filters to your new set before saving it (see "Adding filters to a filter set" on page 15-15).

Select **CANCEL** to leave the Add Filter Set screen without saving the new filter set and return to the Filter Sets screen.

Input and output filters—source and destination

There are two kinds of filters you can add to a filter set: input and output. Input filters check packets received from the Internet, destined for your network. Output filters check packets transmitted from your network to the Internet. You might use output filters, for example to selectively control which users on your network have access to the Internet or to a remote corporate network.

The Netopia R-series Router
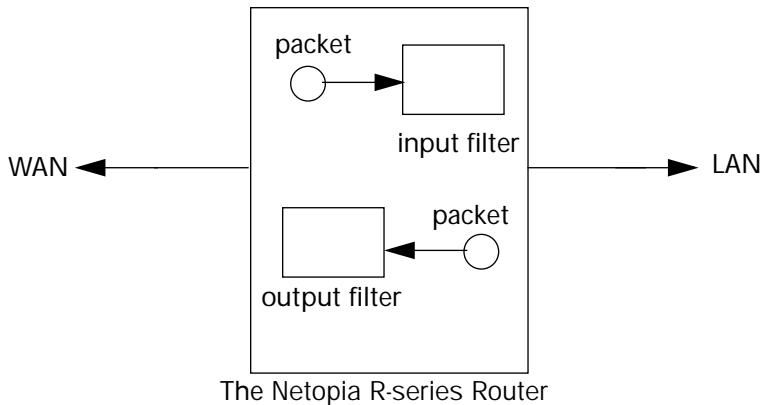
Packets in the Netopia R3100 pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

The process for adding input and output filters is exactly the same. The main difference between the two involves their reference to **source** and **destination**. From the perspective of an input filter, your local network is the **destination** of the packets it checks, and the remote network is their **source**. From the perspective of an output filter, your local network is the **source** of the packets, and the remote network is their **destination**.

Type of filter	"source" means	"destination" means
Input filter	the remote network	the local network
Output filter	the local network	the remote network

Adding filters to a filter set

In this section you'll learn how to add an input filter to a filter set. Adding an output filter works exactly the same way, providing you keep the different source and destination perspectives in mind.

To add an input filter, select **Add Input Filter** in the Add IP Filter Set screen and go to the Add Filter screen. (Select **Add Output Filter** to add an output filter.)

```
                           Add Filter
                  Enabled:                No
                  Forward:                No

                  Source IP Address:      0.0.0.0
                  Source IP Address Mask: 0.0.0.0

                  Dest. IP Address:       0.0.0.0
                  Dest. IP Address Mask:  0.0.0.0

                  Protocol Type:          0

                  Source Port Compare...  No Compare
                  Source Port ID:         0
                  Dest. Port Compare...   No Compare
                  Dest. Port ID:          0

                  ADD THIS FILTER NOW     CANCEL

   Enter the IP specific information for this filter.

```

1. To make the filter active in the filter set, select **Enabled** and toggle it to **Yes**. If **Enabled** is toggled to **No**, the filter can still exist in the filter set, but it will have no effect.

2. If you want the filter to forward packets that match its criteria to the destination IP address, select **Forward** and toggle it to **Yes**. If **Forward** is toggled to **No**, packets matching the filter's criteria will be discarded.

3. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.

4. Select **Source IP Address Mask** and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.

5. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.

6. Select **Dest. IP Address Mask** and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.

7. Select **Protocol Type** and enter **ICMP**, **TCP**, **UDP**, **Any**, or the number of another IP transport protocol (see the table on page 15-9).

   Note: If **Protocol Type** is set to **TCP** or **UDP**, the settings for port comparison that you configure in steps 8 and 9 will appear. These settings only take effect if the Protocol Type is TCP or UDP.

8. Select **Source Port Compare** and choose a comparison method for the filter to use on a packet's source port number. Then select **Source Port ID** and enter the actual source port number to match on (see the table on page 15-8).

9. Select **Dest. Port Compare** and choose a comparison method for the filter to use on a packet's destination port number. Then select **Dest. Port ID** and enter the actual destination port number to match on (see the table on page 15-8).

10. When you are finished configuring the filter, select **ADD THIS FILTER NOW** to save the filter in the filter set. Select **CANCEL** to discard the filter.

Viewing filters

To display a view-only table of input (output) filters, select **Display/Change Input Filters** (**Display/Change Output Filters**) in the Add IP Filter Set screen.

Modifying filters

To modify a filter, select **Display/Change Input Filter** (**Display/ Change Output Filter**) in the Add IP Filter Set screen to display a table of filters.

Select a filter from the table and press Return to go to the Change Filter screen. The parameters in this screen are the same as the ones in the Add Filter screen (see "Adding filters to a filter set" on page 15-15).

```
                         Change Filter

                Enabled:                 No
                Forward:                 No

                Source IP Address:       0.0.0.0
                Source IP Address Mask:  0.0.0.0

                Dest. IP Address:        0.0.0.0
                Dest. IP Address Mask:   0.0.0.0

                Protocol Type:           0

                Source Port Compare...   No Compare
                Source Port ID:          0
                Dest. Port Compare...    No Compare
                Dest. Port ID:           0

  Enter the IP specific information for this filter.


```

Deleting filters

To delete a filter, select **Delete Input Filter** (**Delete Output Filter**) in the Add Filter Set screen to display a table of filters.

Select the filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

Viewing filter sets

To display a view-only list of filter sets, select **Display/Change Filter Sets** in the IP Filter Sets screen.

Modifying filter sets

To modify a filter set, select **Display/Change Filter Set** in the Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to go to the Change IP Filter Set screen. The items in this screen are the same as the ones in the Add Filter screen (see).

```
                        Change IP Filter Set

     Filter Set Name:                  Basic Firewall

     Display/Change Input Filter...
     Add Input Filter...
     Delete Input Filter...


     Display/Change Output Filter...
     Add Output Filter...
     Delete Output Filter...
```

Deleting a filter set

Note: If you delete a filter set, all of the filters it contains are deleted as well. To reuse any of these filters in another set, you'll have to note their configuration before deleting the current filter set and then recreate them.

To delete a filter set, select **Delete Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

A sample IP filter set

This section contains the settings for a filter set, called Basic Firewall, which is part of the Netopia R3100's factory configuration.

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but passes all traffic originating from the LAN. It follows the conservative "that which is not expressly permitted is prohibited" approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall's filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect as filter 4 would have already passed OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly passes all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters pass all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter passes all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

Basic Firewall is suitable for a LAN containing only client hosts that wish to access servers on the WAN, not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly pass WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See "Possible modifications," below, for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes

- Forward: Yes

- Source IP Address: a.b.c.d

- Source IP Address Mask: 255.255.255.255

- Dest. IP Address: 0.0.0.0

- Dest. IP Address Mask: 0.0.0.0

- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes

- Forward: Yes

- Source IP Address: a.b.c.d

- Source IP Address Mask: e.f.g.h

- Dest. IP Address: 0.0.0.0

- Dest. IP Address Mask: 0.0.0.0

- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

■   Enabled: Yes

■   Forward: Yes

■   Source IP Address: 0.0.0.0

■   Source IP Address Mask: 0.0.0.0

■   Dest. IP Address: a.b.c.d

■   Dest. IP Address Mask: 255.255.255.255

■   Protocol Type: TCP

■   Source Port Comparison: No Compare

■   Source Port ID: 0

■   Dest. Port Comparison: Equal

■   Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or 80 for WWW.

AURP tunnel. To allow an AURP tunnel between a remote AURP router with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243) and a local AURP router (including the Netopia R3100 itself), insert the following input filter ahead of the current input filter 1:

■   Enabled: Yes

■   Forward: Yes

■   Source IP Address: a.b.c.d

■   Source IP Address Mask: 255.255.255.255

■   Dest. IP Address: 0.0.0.0

■   Dest. IP Address Mask: 0.0.0.0

■   Protocol Type: UDP

■   Source Port Comparison: Equal

■   Source Port ID: 387

■   Dest. Port Comparison: Equal

■   Dest. Port ID: 387

IPX filters

```
┌──────────┐      ┌─────────────┐      ┌──────────────┐      ┌──────────────┐
│  Main    │      │   System    │      │ Filter Sets  │      │ IPX Filters  │
│  Menu    │ ───▶ │Configuration│ ───▶ │ (Firewalls)  │ ───▶ │and Filter Sets│
└──────────┘      └─────────────┘      └──────────────┘      └──────────────┘
```
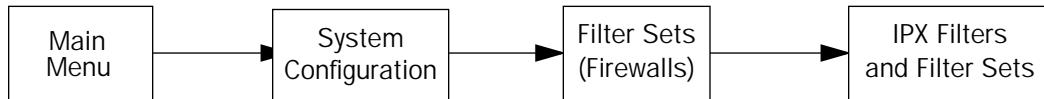
IPX packet filters work very similarly to IP packet filters. They filter data traffic coming from or going to remote IPX networks. IPX filters can be set up to pass or discard IPX packets based on a number of user-defined criteria. Like IP filters, IPX filters must be grouped in sets that are applied to the answer profile or to connection profiles.

IPX SAP filters are used for filtering server entries not required to pass over the WAN links. When connecting to a large IPX network via dial-up connection, the transfer of large numbers of SAP entries can consume significant bandwidth on the WAN link.

Note: Using SAP filtering to prevent a server from being advertised does not provide security against that server being accessed—IPX packet filtering must be used for that purpose.

Setting up and using IPX filter sets is a four-step process:

1. Create the filters to use.

2. Create the filter sets to use.

3. Add filters to the filter sets.

4. Attach the filter sets to the answer profile or to connection profiles.

You can configure IPX filters and set up IPX filter sets from the IPX Filters and Filter Sets screen.

```
┌────────────────────────────────────────────────────────────────────┐
│                                                                      │
│                      IPX Filters and Filter Sets                     │
│                                                                      │
│             Display/Change IPX Packet Filters...                     │
│             Add IPX Packet Filter...                                 │
│             Delete IPX Packet Filter...                              │
│                                                                      │
│             Display/Change IPX Packet Filter Sets...                 │
│             Add IPX Packet Filter Set...                             │
│             Delete IPX Packet Filter Set...                          │
│                                                                      │
│             Display/Change IPX Sap Filters...                        │
│             Add IPX Sap Filter...                                    │
│             Delete IPX Sap Filter...                                 │
│                                                                      │
│             Display/Change IPX Sap Filter Sets...                    │
│             Add IPX Sap Filter Set...                                │
│             Delete IPX Sap Filter Set...                             │
│                                                                      │
│                                                                      │
│                                                                      │
│   Define your filters 1st. IPX Filter Sets refer to, but don't contain, filters. │
│                                                                      │
└────────────────────────────────────────────────────────────────────┘
```

The items in the IPX Filters and Filter Sets screen are grouped into four areas:

■   IPX packet filters

■   IPX packet filter sets

■   IPX SAP filters

■   IPX SAP filter sets

The following sections explain the items in each of these areas.

IPX packet filters

For each IPX packet filter, you can configure a set of parameters to match on the source or destination attributes of IPX data packets coming from or going to the WAN.

Viewing and modifying packet filters

To display a view-only table of IPX packet filters, select **Show/Change IPX Packet Filters** in the IPX Filters and Filter Sets screen.

To modify any of the filters in the table, note the desired filter and press Return to go to the Change Packet Filter screen. The parameters in this screen are the same as the ones in the Add Packet Filter screen (see the next section).

Adding a packet filter

To add a new IPX packet filter, select **Add IPX Packet Filter** in the IPX Filters and Filter Sets screen and press Return to go to the Add Packet Filter screen.

```
                    Add Packet Filter

        Filter Name:                        IPX Filter 1

        Source Network:                     00000000
        Source Node Address:                000000000000
        Source Socket:                      0000

        Destination Network:                00000000
        Destination Node Address:           000000000000
        Destination Socket:                 0000






        ADD FILTER NOW                      CANCEL

   Configure a new IPX Packet Filter. Finished?  ADD or CANCEL to exit.
```

By default, the filter's socket numbers and network and node addresses are null (all zeros). This sets the filter to match on any IPX data packet. You should configure the filter using criteria that meet your security needs.

1. Select **Filter Name** and enter a descriptive name for the filter.

2. To specify a source network for the filter to match on, select **Source Network** and enter an IPX network address.

3. To specify a source node for the filter to match on, select **Source Node Address** and enter an IPX node address.

4. To specify a source socket for the filter to match on, select **Source Socket** and enter an IPX source socket number.

5. To specify a destination network for the filter to match on, select **Destination Network** and enter an IPX network address.

6. To specify a destination node for the filter to match on, select **Destination Node Address** and enter an IPX node address.

7. To specify a destination socket for the filter to match on, select **Destination Socket** and enter an IPX destination socket number.

8. Select **ADD FILTER NOW** to save the current filter. Select **CANCEL** to exit the Add Packet Filter screen without saving the new filter.

Deleting a packet filter

To delete a packet filter, select **Delete IPX Packet Filter** in the IPX Filters and Filter Sets screen to display a table of filters. Select a filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

IPX packet filter sets

Before the individual filters can be used, IPX packet filters must be grouped into sets. A filter can be part of more than one filter set.

Viewing and modifying packet filter sets

To display a table of IPX packet filter sets, select **Show/Change IPX Packet Filter Sets** in the IPX Filters and Filter Sets screen.

To modify any of the filter sets in the list, select the desired filter set and press Return to go to the Change Packet Filter Set screen. The parameters in this screen are the same as the ones in the Add Packet Filter Set screen (see the next section).

Adding a packet filter set

To add a new IPX packet filter set, select **Add IPX Packet Filter Set** in the IPX Filters and Filter Sets screen and press Return to go to the Add Packet Filter Set screen.

```
        Add Packet Filter Set

        Filter Set Name:

        Show Filters/Change Action on Match...

        Append Filter...

        Remove Filter...




        ADD FILTER SET NOW                          CANCEL

   Configure an IPX Filter Set here. You must ADD FILTER SET NOW to save.
```

Follow these steps to configure the new packet filter set:

1. Select **Filter Set Name** and enter a descriptive name for the filter set.

2. To change the forwarding action of filters in the filter set, select **Show Filters/Change Action on Match** and press Return to go to the Show Filters/Change Actions on Match screen.

```
              Show Filters/Change Actions on Match

              Filter Name--------------------Forward

              Filter 1                         No

              Filter 2                         No

              <<NO MATCH>>                     Yes


   Set whether filters forward or drop matching packets here.
```

Select a filter and toggle the packet forwarding action to **Yes** (pass) or **No** (discard).

3. To add a filter to the filter set, select **Append Filter** to display a table of filters. Select a filter from the table and press Return to add it to the filter set. The default action of newly added filters is to *not* forward packets that match their criteria.

    To exit the table without adding the filter, press the Escape key.

4. To remove a filter from the filter set, select **Detach Filter** to display a table of appended filters. Select a filter from the table and press Return to remove it from the set. To exit the table without removing the filter, press the Escape key.

5. Select **ADD FILTER SET NOW** to save the current filter set. Select **CANCEL** to exit the Add Packet Filter Set screen without saving the new filter set.

Deleting a packet filter set

To delete a packet filter set, select **Delete IPX Packet Filter Set** in the IPX Filters and Filter Sets screen to display a list of filter sets. Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

Note: Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

IPX SAP filters

For each IPX SAP filter, you can configure a set of parameters to match on certain attributes of IPX SAP packet entries. The filters check IPX SAP packets for entries that match and then act on those entries. The SAP packets themselves are always allowed to continue after their entries are checked.

The purpose of filtering SAP packets is not to make your network more secure, but to add efficiency to network bandwidth use. Filtering SAP packets may reduce the size of SAP packets and SAP bindery tables by removing unwanted entries.

Viewing and modifying SAP filters

To display a table of IPX SAP filters, select **Show/Change IPX SAP Filters** in the IPX Filters and Filter Sets screen.

To modify any of the filters in the table, select the desired filter and press Return to go to the Change SAP Filter screen. The parameters in this screen are the same as the ones in the Add SAP Filter screen (see the next section).

Adding a SAP filter

To add a new IPX SAP filter, select **Add IPX SAP Filter** in the IPX Filters and Filter Sets screen and press Return to go to the Add SAP Filter screen.

```
                      Add Sap Filter

          Filter Name:

          Server Name:

          Socket:                              0000

          Type:                                0000

          IPX Network:                         00000000
          IPX Node Address:                    000000000000




          ADD FILTER NOW                       CANCEL

     Configure a new IPX SAP Filter. Finished?  ADD or CANCEL to exit.


```

By default, the filter's socket and type numbers and network and node addresses are null (all zeros). This sets the filter to match on any IPX SAP packet entry. You should configure the filter using criteria that meet your needs.

Follow these steps to configure the new SAP filter:

1. Select **Filter Name** and enter a descriptive name for the filter.

2. To specify a server name for the filter to match on, select **Server Name** and enter the name of an IPX server. You can use the wildcard characters * (asterisk) and ? (question mark). Use * to match any string, including a null string (no characters), and ? to match any single character in the server's name. For example, the filter could match on the server name "NETOPIA" with "NETO*", "NETO?IA", and "NETOPIA*".

3. To specify a socket for the filter to match on, select **Socket** and enter an IPX socket number.

4. To specify a type number for the filter to match on, select **Type** and enter an IPX type number.

5. To specify an IPX network address for the filter to match on, select **IPX Network** and enter an IPX network address.

6. To specify an IPX node address for the filter to match on, select **IPX Node Address** and enter an IPX node address.

7. Select **ADD FILTER NOW** to save the current filter. Select **CANCEL** to exit the Add SAP Filter screen without saving the new filter.

Deleting a SAP filter

To delete a SAP filter, select **Delete IPX SAP filter** in the IPX Filters and Filter Sets screen to display a table of filters. Select a filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

IPX SAP filter sets

Before IPX SAP filters can be used, they must be grouped into sets. A SAP filter can be part of more than one filter set.

Viewing and modifying SAP filter sets

To display a table of IPX SAP filter sets, select **Show/Change IPX SAP Filter Sets** in the IPX Filters and Filter Sets screen to display a list of filter sets.

To modify any of the filter sets in the list, select the desired filter set and go to the Change SAP Filter Set screen. The parameters in this screen are the same as the ones in the Add SAP Filter Set screen (see the previous section).

Adding a SAP filter set

To add a new IPX SAP filter set, select **Add IPX SAP Filter Set** in the IPX Filters and Filter Sets screen and go to the Add SAP Filter Set screen.

```
          Add SAP Filter Set


          Filter Set Name:

          Show Filters/Change Action on Match...

          Append Filter...

          Remove Filter...





          ADD FILTER SET NOW                    CANCEL
    Configure an IPX Filter Set here. You must ADD FILTER SET NOW to save.

```
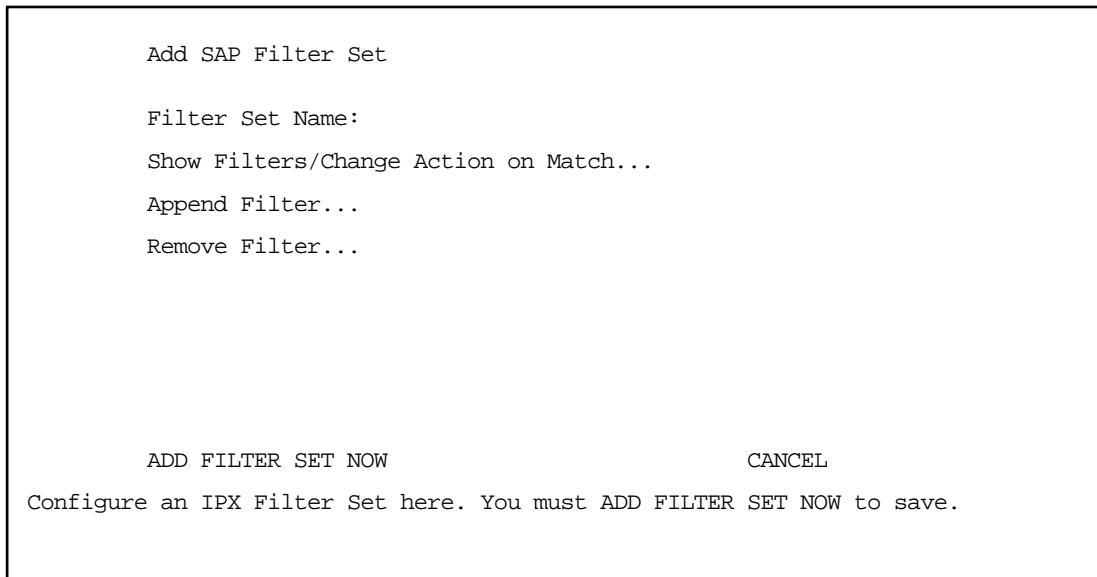
Follow these steps to configure the new SAP filter set:

1. Select **Filter Set Name** and enter a descriptive name for the filter set.

2. To change the forwarding action of filters in the filter set, select **Show Filters/Change Action on Match** and press Return to go to the Show Filters/Change Actions on Match screen.

```
                    Show Filters/Change Actions on Match

              Filter Name--------------------Forward

              Filter 1                             No

              Filter 2                             No

              <<NO MATCH>>                         Yes

 Set whether filters forward or drop matching packets here.
```

Select a filter and toggle the entry forwarding action to **Yes** (pass) or **No** (discard).

3. To add a filter to the filter set, select **Append Filter** to display a table of filters. Select a filter from the table and press Return to add it to the filter set. The default action of newly added filters is to *not* forward (discard) packet entries that match their criteria.

    To exit the table without adding the filter, press the Escape key.

4. To remove a filter from the filter set, select **Detach Filter** to display a table of appended filters. Select a filter from the table and press Return to remove it from the set. To exit the table without removing the filter, press the Escape key.

5. Select **ADD FILTER SET NOW** to save the current filter set. Select **CANCEL** to exit the Add SAP Filter Set screen without saving the new filter set.

Deleting a SAP filter set

To delete a SAP filter set, select **Delete IPX SAP Filter Set** in the IPX Filters and Filter Sets screen to display a list of filter sets. Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

Note: Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

Firewall tutorial

General Firewall Terms

Firewall: a component or set of components that restrict access between a protected network and the Internet, or between two networks.

Host: A workstation on the Network.

Packet: Unit of communication on the Internet.

Packet Filter: Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports, or the TCP ACK bit.

Port: A number that defines a particular type of service.

Filter Rule: A filter set is comprised of individual filter rules.

Filter Set: A grouping of individual filter rules.

Basic IP Packet Components

All IP packets contain the same basic "header" information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27
Source Port	2541
Destination Port	80
Protocol	TCP
ACK Bit	Yes
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that a packet filter does not look into the IP datastream (the User Data from above) to make filtering decisions.

Basic Protocol Types

TCP: Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.

UDP: User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not re transmit the data. RFC 768 is the specification for UDP.

And there are many more ports defined in the Assigned Addresses RFC.

Example TCP/UDP Ports

TCP Port	Service	UDP Port	Service
20/21	FTP	161	SNMP
23	Telnet	69	TFTP
25	SMTP	387	AURP
80	WWW		
144	News		

Firewall design rules

There are two basic rules to firewall design:

■   "What is not explicitly allowed is denied..."

and

■   "What is not explicitly denied is allowed..."

The first rule is far more secure, and is the best approach to firewall design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and future.

Firewall Logic

Firewall design is a test of logic, and filter rule ordering is critical. If a packet is passed through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not pass through the remainder of the filter rules.

For example, if you had the following filter set...

    Allow WWW access;

    Allow FTP access;

    Allow SMTP access;

    Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first rule (WWW), go through the second rule (FTP), matches this rule and the packet is allowed through.

If you had this filter set for example....

    Allow WWW access;

    Allow FTP access;

    Deny FTP access;

    Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first filter rule (WWW), match the second rule (FTP) and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Binary Representation

It is easiest when doing filtering to convert the IP address and mask in question to binary. This will allow you to perform the logical AND to determine if a packet matches a filter rule.

Logical ANDing

When a packet is compared (in most cases) a logical AND is performed. First the IP addresses and subnet masks are converted to binary and then ANDed together. The rules for logical ANDing are as follows:

    0 AND 0 = 0

    0 AND 1 = 0

    1 AND 0 = 0

    1 AND 1 = 1

For example:

Filter rule:

    Deny

    IP: 163.176.1.15   BINARY: 10100011.10110000.00000001.00001111

    Mask: 255.255.255.255   BINARY: 11111111.11111111.11111111.11111111

Incoming Packet:

    IP 163.176.1.15   BINARY: 10100011.10110000.00000001.00001111

AND the incoming packet and subnet mask together, the result is:

$$10100011.10110000.00000001.00001111$$

which matches the IP address in the filter rule and the packet is denied.

Implied Rules

With a given set of filter rules, there is an Implied rule which may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied is NO.
N+N+N=Y	If all filter rules are NO, the implied is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied is NO.

Established Connections

The TCP header contains one bit called the ACK Bit (or TCP Ack bit). This ACK Bit only appears with TCP, not UDP. The ACK bit is part of the TCP mechanism that guaranteed the delivery of data. The ACK bit is set whenever one side of a connection has received data from the other side. Only the first TCP packet will not have the ACK bit set, once the TCP connection is in place the remainder of the TCP packets with have the ACK bit set.

The ACK bit is helpful for firewall design and reduces the number of potential filter rules. A filter rule could be created just allowing incoming TCP packets with the ACK bit set, as these packets had to be originated from the local network.

Example IP Filter Set Screen

This is an example of the Netopia IP filter set screen:

```
                          Change Filter
          Enabled:                         Yes
          Forward:                         No

          Source IP Address:               0.0.0.0
          Source IP Address Mask:          0.0.0.0

          Dest. IP Address:                0.0.0.0
          Dest. IP Address Mask:           0.0.0.0

          Protocol Type:                   TCP

          Source Port Compare...           No Compare
          Source Port ID:                  0
          Dest. Port Compare...            Equal
          Dest. Port ID:                   2000
          Established TCP Conns. Only:     No



  Return/Enter accepts * Tab toggles * ESC cancels.
  Enter the IP specific information for this filter.
```

Filter Basics

In the source or destination IP address fields, the IP address that is entered MUST be the NETWORK address of the subnet. A HOST address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

The Netopia R3100 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined

Less Than Or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined.

Example Network
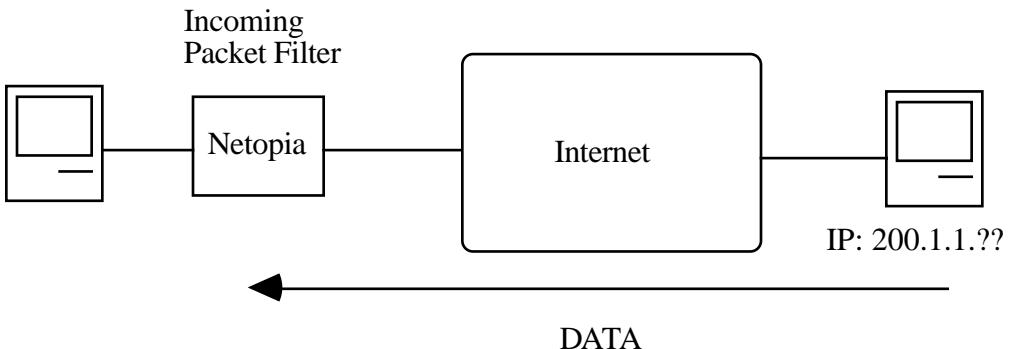
Example Filters

Example 1

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

IP Address	Binary Representation	
200.1.1.28	00011100	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	00000000	(Logical AND result)

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field (00000000) in the Netopia R3100. This will NOT forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	10000000	(Logical AND result)

This incoming IP packet (10000000) has a source IP address that does not match the network address in the Source IP Address field (00000000) in the Netopia R3100. This rule WILL forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	10110000	(Logical AND result)

Since the Source IP Network Address in the Netopia R3100 is 01100000, and the source IP address after the logical AND is 1011000, this rule does NOT match and this packet will be passed.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104

IP Address	Binary Representation	
200.1.1.104	01101000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R3100 is 01100000, and the source IP address after the logical AND is 01100000, this rule DOES match and this packet will NOT be passed.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96

IP Address	Binary Representation	
200.1.1.96	01100000	(Source address in incoming IP packet)
AND		
255.255.255.255	11111111	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R3100 is 01100000, and the source IP address after the logical AND is 01100000, this rule DOES match and this packet will NOT be passed. This rule masks off a SINGLE IP address.

Token Security Authentication

This section discusses how to configure and use security authentication on the Netopia R3100.

Note: The security authentication feature only applies to Netopia R3100 models connecting over a dial-up line using the PPP-PAP-TOKEN or PPP-CACHE-TOKEN authentication protocol.

Securing network environments

Unauthorized tampering or theft of information on internal networks causes serious ramifications, given the reliance on information systems. Network abuse is a serious problem, complicated by the difficulty in detecting the source of the abuses. An unauthorized user can gain access to networks and copy information without leaving a trace.

Password protection is one solution, but static passwords are often insecure. They can be compromised, allowing unauthorized users to disguise themselves as authorized users and enter supposedly secure systems. However, a company called Security Dynamics™ has patented a security authentication technology to increase network security.

SecurID is a two-factor authentication process to protect against unauthorized access. This dynamic user authentication produces a randomly-generated security code mechanism that changes every 60 seconds. At login, authorized users enter their password and the code displayed on their SecurID token card. While a password may be compromised, the constantly changing access code, which requires the token card during system use, bars unauthorized users from entering the network.

Using the SecurID token card

Each SecurID token card is programmed with an algorithm that ensures every code displayed is valid only for that user at that particular time. The token card has a display that authorizes the individual user access to the computer. Through this authentication system, the user's identity is verified when the correct password and current code are entered from the user's token.

Personal identification number (PIN)

The user's password is called a personal identification number, or PIN. The user enters the secret PIN from a console connection, followed by the current code displayed on the token card. Then the access control module must authenticate the token's unique code in combination with the user's secret PIN before access is granted.

Key Security Authentication Features of the Netopia R3100

As a remote device, the Netopia R3100 offers client/calling side security authentication. This feature allows the Netopia R3100 to call a server router and perform security card authentication. The router of the called server must have access to a server with ACE software loaded on it.

To perform security card authentication, each user must have a security authentication token card and a PIN. In addition, the user's identifying information must reside on the remote ACE servers for authentication negotiation to properly take place.

The Netopia R3100 supports the following user configurations for security authentication:

■   Single user, calling a single destination (single session)

■   Single user, calling multiple destinations (two simultaneous and separate sessions)

■   Multiple users, calling a single destination (single session)

■   Multiple users, calling multiple destinations (two simultaneous and separate sessions

Security authentication components

To properly identify and authenticate an authorized user, the following are required:

■   A secret personal identification number (PIN) for each user.

■   A security authentication token card.

■   A Security Access Control Module (ACM).

Note: The Netopia R3100 currently only supports Ascend routers as ACMs.

■   An external Netopia R3100 calling into a designated server. For example, a telecommuter dialing into a remote site from a Netopia R3100 interested in accessing personal email or file sharing services.

Note: The Netopia R3100 does not include a security authentication token card.

Configuring for security authentication

To configure the Netopia R3100 to support security authentication, select an authentication method and set up a designated connection profile from the System Configuration screen or your first connection profile from Easy Setup.

1.   From the WAN Configuration menu, select Display/Change Connection Profile. From the pop-up menu that appears, select a Connection Profile. In the Connection Profile screen select **Datalink Options**.

```
┌──────────┐      ┌──────────────┐      ┌──────────────────┐      ┌──────────────────┐
│   Main   │ ───▶ │     WAN      │ ───▶ │  Display/Change  │ ───▶ │ Datalink Options │
│   Menu   │      │ Configuration│      │Connection Profile│      │                  │
└──────────┘      └──────────────┘      └──────────────────┘      └──────────────────┘
```
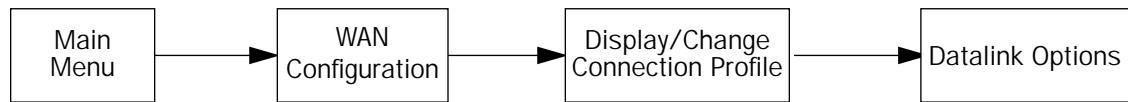
```
                        Datalink (PPP/MP) Options


        Data Compression...                        Ascend LZS

        Send Authentication...                     PAP-TOKEN

        Send User Name:


        Receive User Name:
        Receive Password:

        Channel Usage...                           Dynamic

        Bandwidth Allocation...                    Auto

        Maximum Packet Size:                       1500



   In this Screen you will configure the PPP/MP specific connection params.
```

2. Select Send Authentication and press Return. From the pop-up menu, highlight **PAP-TOKEN** or
    CACHE-TOKEN. Your network administrator or the remote network administrator will tell you which method
    to select.

    If you select PAP-TOKEN, select **Send User Name** and enter a name for your Netopia R3100. You will not
    need to enter a Send Password for PAP-TOKEN. Press Return.

    If you select CACHE-TOKEN, select **Send User Name** and enter a name for your Netopia R3100. Then,
    select **Send Password** and enter a secret name or number. Press Return.

3. Set up a connection profile to use with your authentication method. For information on setting up a
    connection profile, see Chapter 7, "Easy Setup."

Note: If you are setting up your first connection profile, you can also enter your authentication information in
the Easy Setup Connection Profile screen.

Connecting using security authentication

You can initiate a connection call using security authentication in either of two ways:

■   establish a dial-on-demand (DOD) connection, or

■   establish a manual connection.

Establishing a dial-on-demand (DOD) connection call

To establish a connection call using DOD, select Utilities & Diagnostics from the Main Menu and press Return.

Note: The Secure Authentication Monitor field will remain hidden if PAP-TOKEN or CACHE-TOKEN is not the
selected authentication method in the connection profile.

```
                     Utilities & Diagnostics


              Ping...
              Trace Route...


              Call Accounting...
              Secure Authentication Monitor...


              Trivial File Transfer Protocol (TFTP)...
              X-Modem File Transfer...



              Revert to Factory Defaults...

              Restart System...
```

1. Select **Secure Authentication Monitor** and press Return. The Secure Authentication Monitor screen appears.

2. Wait for the call to initiate.

```
               Secure Authentication Monitor


                    Current Connection Status
    Profile Name---State---%Use---Remote Address---Est.---More Info---


    Status --- Passcode Required

    For Connection Profile:  Easy Setup Profile

    0-Challenge: Enter PASSCODE:
    Passcode:                123412345678
```

3. From the fields that appear, select **Enter PASSCODE** and press Return. Enter your PIN and the code displayed on your security authentication token card LED.

4. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one connection, you will be prompted for each connection being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

When using PAP-TOKEN, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

Establishing a manual connection call

To establish a Manual connection call, select WAN Configuration from the Main Menu and press Return.

1. Select **Establish WAN Connection** from the WAN Configuration screen and press Return. The Establish WAN Connection screen displays a table of all of the connection profiles you have defined. Highlight the connection profile you wish to manually call. Press Return to initiate the call.

```
                         Call Status

                 Profile Name -- Easy Setup Profile
                 Connection State -- Dialing

                 Channel 1 State  -- Acquiring

                 Channel 2 State  --


 0-Challenge: Enter PASSCODE:
 Passcode:                    123412345678


Hit ESCAPE/RETURN/ENTER to return to previous menu.
```
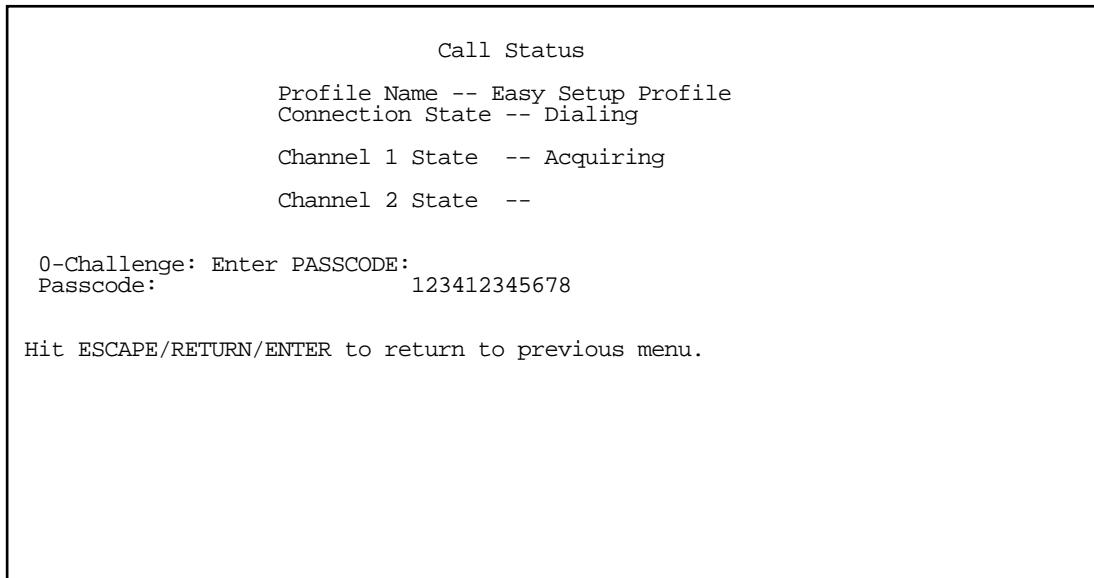
2. From the fields that appear, select **Enter PASSCODE** and press Return. Enter your PIN and the code displayed on your security authentication token card LED screen.

3. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one connection, you will be prompted for each channel being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

When using PAP-TOKEN for a dial-up call, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

Chapter 16

Utilities and Diagnostics

A number of utilities and tests are available for system diagnostic and control purposes:

- "Ping" on page 16-2
- "Telnet client" on page 16-4
- "Trace Route" on page 16-5
- "Secure Authentication Monitor" on page 16-6
- "Disconnect Telnet Console Session" on page 16-7
- "Transferring configuration and firmware files with TFTP" on page 16-7
- "Transferring configuration and firmware files with XMODEM" on page 16-10
- "Factory defaults" on page 16-7
- "Restarting the system" on page 16-12
- "ISDN Switch Loopback Test" on page 16-13

Note: These utilities and tests are accessible only through the console-based management screens. See Chapter 6, "Console-based Management," for information on accessing the console-based management screens.

You access the **Utilities & Diagnostics** screens from the **Main Menu**.

```
              Utilities & Diagnostics


        Ping...
        Trace Route...


        Call Accounting...
        Secure Authentication Monitor...


        Trivial File Transfer Protocol (TFTP)...
        X-Modem File Transfer...



        Revert to Factory Defaults...

        Restart System...

        ISDN Switch Loopback Test...
```
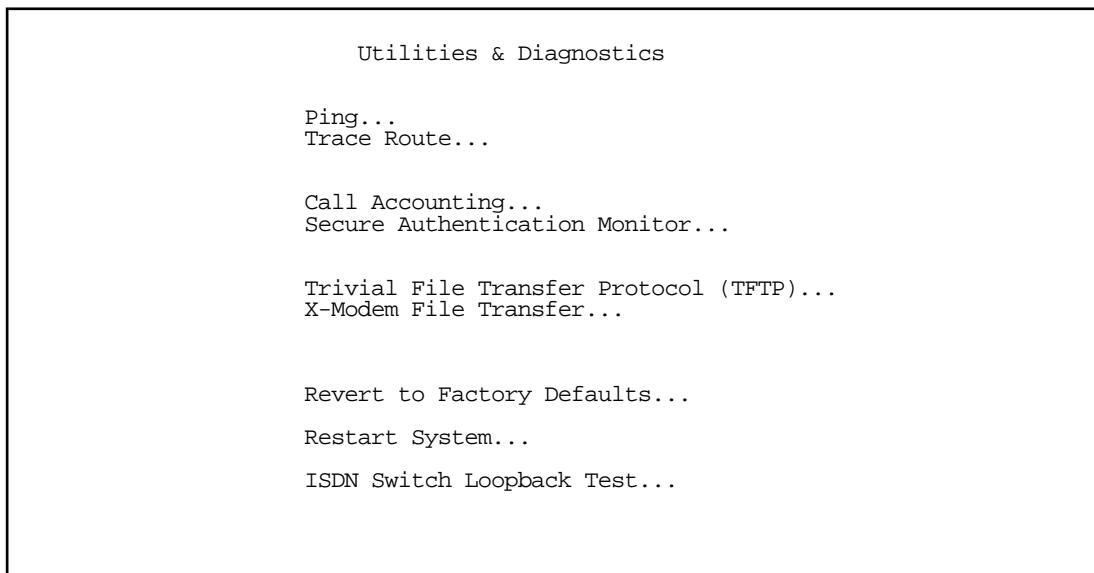
Ping

The Netopia R3100 includes a standard Ping test utility. A Ping test generates IP packets destined for a particular (Ping-capable) IP host. Each time the target host receives a Ping packet, it returns a packet to the original sender.

Ping allows you to see whether a particular IP destination is reachable from the Netopia R3100. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

To use the Ping utility, select **Ping** in the Statistics, Utilities, Tests screen and press Return to go to the Ping screen.

```
                              ICMP Ping

          Name of Host to Ping:
          Packets to Send:                    5
          Data Size:                          56
          Delay (seconds):                    1

                             START PING


          Status:

          Packets Out:                        0
          Packets In:                         0
          Packets Lost:                       0 (0%)
          Round Trip Time
            (Min/Max/Avg):                    0.000 / 0.000 / 0.000 secs


     Enter the IP Address/Domain Name of a host to ping.
     Send ICMP Echo Requests to a network host.


```

To configure and initiate a Ping test, follow these steps:

1. Select **Name of Host to Ping** and enter the destination domain name or IP address.

2. Select **Packets to Send** to change the default setting. This is the total number of packets to be sent during the Ping test. The default setting is adequate in most cases, but you may change it to any value from 1 to 4,294,967,295.

3. Select **Data Size** to change the default setting. This is the size, in bytes, of each Ping packet sent. The default setting is adequate in most cases, but you may change it to any value from 0 (only header data) to 1664.

4. Select **Delay (seconds)** to change the default setting. The delay, in seconds, determines the time between Ping packets sent. The default setting is adequate in most cases, but you may change it to any value from 0 to 4,294,967. A delay of 0 seconds forces packets to be sent immediately one after another.

5. Select **START PING** and press Return to begin the Ping test. While the test is running, the **START PING** item becomes **STOP PING**. To manually stop the Ping test, select **STOP PING** and press Return or the Escape key.

While the Ping test is running, and when it is over, a status field and a number of statistical items are active on the screen. These are described below.

Status: The current status of the Ping test. This item can display the following messages:

Message	Description
Resolving host name	Finding the IP address for the domain name-style address
Can't resolve host name	IP address can't be found for the domain name-style name
Pinging	Ping test is in progress
Complete	Ping test was completed
Cancelled by user	Ping test was cancelled manually
Destination unreachable from w.x.y.z	Ping test was able to reach the router with IP address w.x.y.z, which reported that the test could not reach the final destination
Couldn't allocate packet buffer	Couldn't proceed with Ping test; try again or reset system
Couldn't open ICMP port	Couldn't proceed with Ping test; try again or reset system

Packets Out: The number of packets sent by the Ping test.

Packets In: The number of return packets received from the target host. To be considered "on time," return packets are expected back before the next packet in the sequence of Ping packets is sent. A count of the number of late packets appears in parentheses to the right of the **Packets In** count.

In the example below, a Netopia R3100 is sending Ping packets to another host, which responds with return Ping packets. Note that the second return Ping packet is considered to be late because it is not received by the Netopia R3100 before the third Ping packet is sent. The first and third return Ping packets are on time.
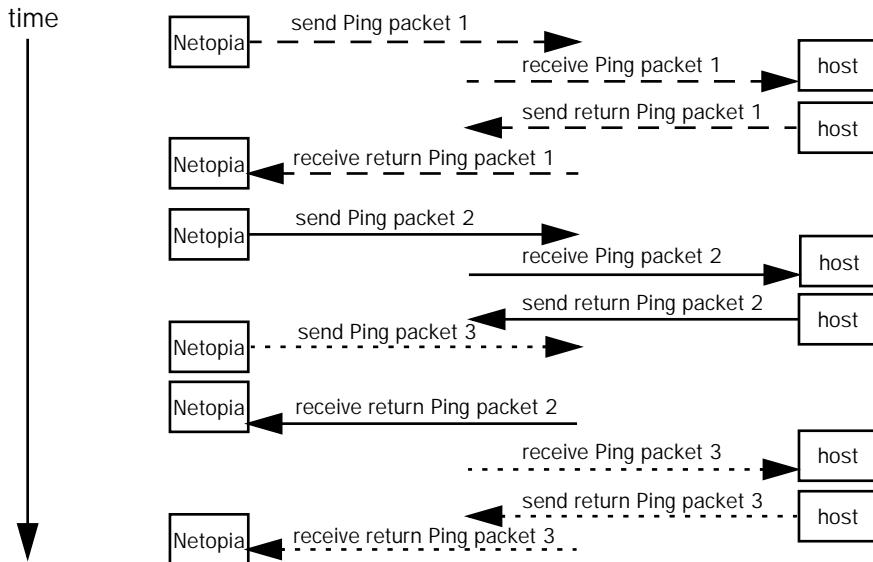
Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between **Packets Out** and **Packets Lost**, and **Packets In** is noticeably lagging behind **Packets Out**, the destination is probably unreachable. In this case, use **STOP PING**.

Round Trip Time (Min/Max/Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Netopia R3100 is 255, the maximum allowed. The TTL value defines the number of IP routers that the packet can traverse. Ping packets that reach their TTL value are dropped, and a "destination unreachable" notification is returned to the sender (see the table above). This ensures that no infinite routing loops occur. The TTL value can be set and retrieved using the SNMP MIB-II ip group's ipDefaultTTL object.

Telnet client

The Telnet client mode replaces the normal menu mode. Telnet sessions can be cascaded, that is, you can initiate a Telnet client session when using a Telnet console session. To activate the Telnet client, select **Telnet** from the Utilities & Diagnostics menu.

The Telnet client screen appears.

```
                            Telnet
        Host Name or IP Address:

        Control Character to Suspend:      Q

                        START A TELNET SESSION








 Enter the IP Address/Domain Name of a host.


```
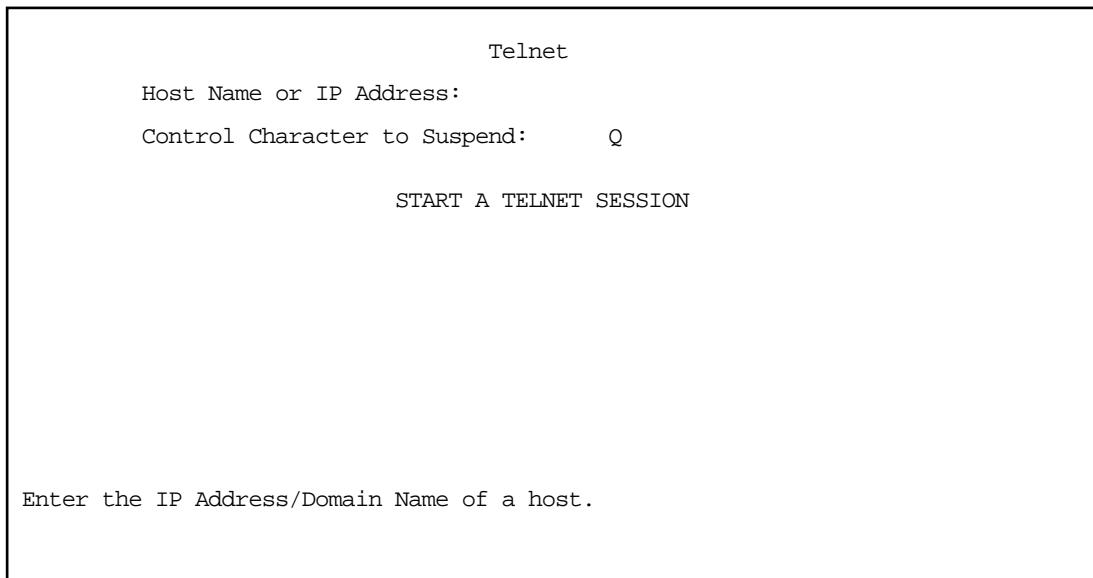
■   Enter the host name or the IP address in dotted decimal format of the machine you want to telnet into and press Return.

■   Either accept the default control character "Q" used to suspend the Telnet session, or type a different one.

■   **START A TELNET SESSION** becomes highlighted.

■   Press Return and the Telnet session will be initiated.

■   To suspend the session, press Control-Q, or whatever other control character you specified.

Two new options will appear in the Telnet screen (not shown):

Resume Suspended Session – select this one if you want to go back to your Telnet session

Terminate Suspended Session – select this one if you want to end the session

Trace Route

You can count the number of routers between your Netopia Router and a given destination with the Trace Route utility.

Select **Trace Route** in the Statistics & Diagnostics screen and press Return to go to the Trace Route screen.

```
                              Trace Route


              Host Name or IP Address:



              Maximum Hops:                 30

              Timeout (seconds):            5



              Use Reverse DNS:              Yes



                         START TRACE ROUTE


 Trace route to a network host.
```

To trace a route, follow these steps:

1. Select **Host Name or IP Address** and enter the name or address of the destination you want to trace.

2. Select **Maximum hops (1..64)** to set the maximum number of routers to count between the Netopia Router and the destination router, up to the maximum of 64. The default is 30 hops.

3. Select **Timeout per probe (1..10 sec)** to set when the trace will timeout for each hop, up to 10 seconds. The default is 3 seconds.

4. Select **Use Reverse DNS** to learn the names of the routers between the Netopia Router and the destination router. The default is Yes.

5. Select **START TRACE ROUTE** and press Return. The screen will be replaced by a scrolling screen, listing the destination, the number of hops, the IP addresses of each hop, and the DNS names, if selected.

6. Cancel the trace by pressing Escape. Return to the Trace Route screen by pressing Escape twice.

Secure Authentication Monitor

Note: The Secure Authentication Monitor field will remain hidden if PAP-TOKEN or CACHE-TOKEN is not the selected authentication method in the Connection Profile.

You use the Secure Authentication Monitor screen when placing one type of SecurID connection call. See for details.

Disconnect Telnet Console Session

If you want to close your Telnet Console session, select **Disconnect Telnet Console Session** and press Return.
A dialog box appears asking you to cancel or continue your selection.

```
                     Utilities & Diagnostics


         +-------------------------------------------------------+
         +-------------------------------------------------------+
         |                                                       |
         |  Are you sure you want to close this Console Session?  |
         |       CANCEL                       CONTINUE           |
         |                                                       |
         |                                                       |
         +-------------------------------------------------------+
                  X-Modem File Transfer...

                  Revert to Factory Defaults...

                  Restart System...
```
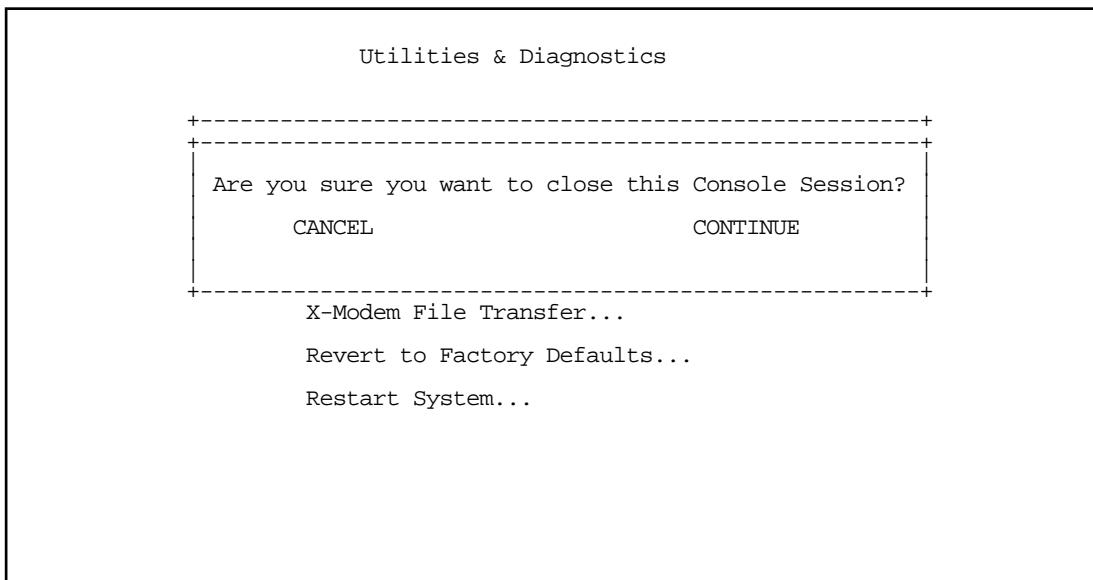
If you select **Continue**, you will immediately terminate your session.

Factory defaults

You can reset the Netopia R3100 to its factory default settings. Select the **Revert to Factory Defaults** item in the Statistics & Diagnostics screen and press Return. Select **CONTINUE** in the dialog box and press Return. The Netopia R3100 will reboot and its settings will return to the factory defaults, deleting your configurations.

In an emergency, you can also use the Reset Switch to return the router to its factory default settings. Call Netopia Tech Support for instructions on using the Reset Switch.

Note: Reset to factory defaults with caution. You will need to reconfigure all your settings in the router.

Transferring configuration and firmware files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the Router as the client. To use the Router as a TFTP client, a TFTP server must be available. Netopia, Inc. has a public access TFTP server on the Internet where you can obtain the latest firmware versions.

To use TFTP, select **Trivial File Transfer Protocol (TFTP)** in the Statistics & Diagnostics screen and press Return to go to the Trivial File Transfer Protocol (TFTP) screen.

```
                    Trivial File Transfer Protocol (TFTP)


        TFTP Server Name:


        Firmware File Name:


        GET ROUTER FIRMWARE FROM SERVER...


        Config File Name:

        GET CONFIG FROM SERVER...
        SEND CONFIG TO SERVER...


        TFTP Transfer State -- Idle

        TFTP Current Transfer Bytes -- 0
```

The sections below describe how to update the Router's firmware and how to download and upload configuration files.

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administrator.

The router firmware governs how the router communicates with your network and with the remote site. Router firmware updates are periodically posted on the Netopia website.

To update the router's firmware, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.

- Select **Firmware File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).

- Select **Send Firmware to Netopia from TFTP Server** and press Return. You will see the following dialog box:
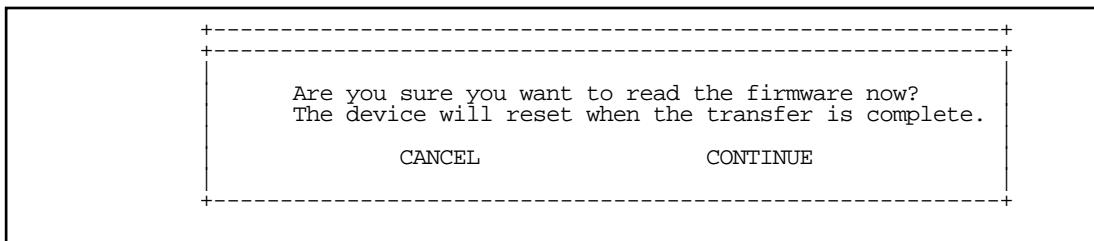
```
        +-----------------------------------------------------------+
        +-----------------------------------------------------------+
        |                                                           |
        |      Are you sure you want to read the firmware now?       |
        |      The device will reset when the transfer is complete.  |
        |                                                           |
        |            CANCEL                    CONTINUE             |
        |                                                           |
        +-----------------------------------------------------------+
```

- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system

will reset at the end of the file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

■ Be sure the firmware update you load onto your router is the correct version for your particular model. Some models do not support all firmware versions. Loading an incorrect firmware version can permanently damage the unit.

■ Do not manually power down or reset the Netopia R3100 while it is automatically resetting or it could be damaged.

■ If you choose to download the firmware, the **TFTP Transfer State** item will change from **Idle** to **Reading Firmware**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Downloading configuration files

The Router can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the Router's parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

■ Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.

■ Select **Config File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).

■ Select **Read Config Now** and press Return. You will see the following dialog box:
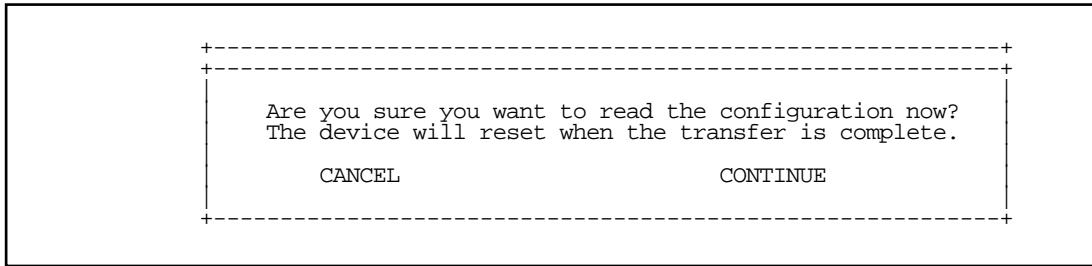
```
        +------------------------------------------------------+
        +------------------------------------------------------+
        |                                                      |
        |     Are you sure you want to read the configuration now?  |
        |     The device will reset when the transfer is complete.  |
        |                                                      |
        |        CANCEL                        CONTINUE        |
        |                                                      |
        +------------------------------------------------------+
```

■ Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new configuration into effect.

■ If you choose to download the configuration file, the **TFTP Transfer State** item will change from **Idle** to **Reading Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Uploading configuration files

Using TFTP, you can send a file containing a snapshot of the Router's current configuration to a TFTP server. The file can then be downloaded by a different Netopia R3100 unit to configure its parameters (see "Downloading configuration files" on page 16-9). This is useful for configuring a number of Routers with identical parameters, or just for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R3100 unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.

2. Select **Config File Name** and enter a name for the file you will upload. The file will appear with the name you choose on the TFTP server. You may need to enter a file path along with the file name (for example, Mypc/Netopia/myfile).

3. Select **Write Config Now** and press Return. Netopia will begin to transfer the file.

4. The **TFTP Transfer State** item will change from **Idle** to **Writing Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Transferring configuration and firmware files with XMODEM

You can transfer configuration and firmware files with XMODEM through the Netopia R3100's console port. Be sure your terminal emulation program supports XMODEM file transfers.

To go to the **X-Modem File Transfer** screen, select it in the Utilities & Diagnostics screen.

Note: The X-Modem File Transfer screen is only available if you are connected via the Console port.

```
                    X-Modem File Transfer


    Send Firmware to Netopia...

    Send Config to Netopia...

    Receive Config from Netopia...
```

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administration.

Follow these steps to update the Netopia R3100's firmware:

1.   Make sure you have the firmware file on disk and know the path to its location.

2.   Select **Send Firmware to Netopia** and press Return. The following dialog box appears:

```
+------------------------------------------------------------------------+
+------------------------------------------------------------------------+
|                                                                        |
|   Are you sure you want to send a firmware file to your Netopia?       |
|   If so, when you hit Return/Enter on the CONTINUE button, you will    |
|   have 10 seconds to begin the transfer from your terminal program.    |
|                                                                        |
|         CANCEL                              CONTINUE                    |
|                                                                        |
+------------------------------------------------------------------------+
```

3.   Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

   If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the firmware file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

   The system will reset at the end of a successful file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

   Do not manually power down or reset the Netopia R3100 while it is automatically resetting or it could be damaged.

Downloading configuration files

The Netopia R3100 can be configured by downloading a configuration file. The downloaded file reconfigures all of the Router's parameters.

Configuration files are available from a site maintained by your organization's network administrator or from your local site (see "Uploading configuration files," below).

Follow these steps to download a configuration file:

1.   Make sure you have the configuration file on disk and know the path to its location.

2.   Select **Send Config to Netopia** and press Return. The following dialog box appears:

```
+------------------------------------------------------------------------+
+------------------------------------------------------------------------+
|                                                                        |
|   Do you want to send a saved configuration to your Netopia?           |
|   If so, when you hit Return/Enter on the CONTINUE button, you will    |
|   have 10 seconds to begin the transfer from your terminal program.    |
|         CANCEL                              CONTINUE                    |
|                                                                        |
+------------------------------------------------------------------------+
```

3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

The system will reset at the end of a successful file transfer to put the new configuration into effect.

Uploading configuration files

A file containing a snapshot of the Netopia R3100's current configuration can be uploaded from the Router to disk. The file can then be downloaded by a different Netopia R3100 to configure its parameters (see "Downloading configuration files" on page 16-11). This is useful for configuring a number of Routers with identical parameters, or for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R3100 by Netopia or your network administrator.

To upload a configuration file:

1. Decide on a name for the file and a path for saving it.

2. Select **Receive Config from Netopia** and press Return. The following dialog box appears:

```
        +-------------------------------------------------------------------+
        |                                                                   |
        |   Are you sure you want to save your current Netopia configuration? |
        |   If so, when you hit Return/Enter on the CONTINUE button, you will |
        |   have 10 seconds to begin the transfer from your terminal program. |
        |                                                                   |
        |           CANCEL                             CONTINUE             |
        |                                                                   |
        +-------------------------------------------------------------------+
```
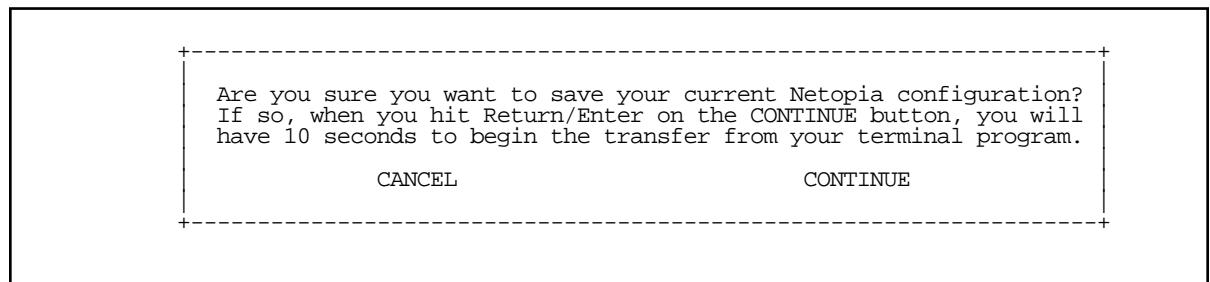
3. Select **CANCEL** to exit without uploading the file, or select **CONTINUE** to upload the file.

If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

Restarting the system

You can restart the system by selecting the **Restart System** item in the Utilities & Diagnostics screen.

You must restart the system whenever you reconfigure the Netopia R3100 and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions. Some configuration processes automatically restart the system to apply the changes you have made.

ISDN Switch Loopback Test

The ISDN loopback test is designed to confirm the existence of a working ISDN line and the proper configuration of certain Netopia R3100 ISDN Router parameters. This test is available only on switched ISDN lines.

Using the first B-channel, the test calls the Netopia R3100 on the second B-channel, creating a call loop back to the unit.

To run the ISDN loopback test, select **ISDN Switch Loopback Test** in the Utilities & Diagnostics screen and press Return. The ISDN Switch Loopback Test screen appears.

```
                          ISDN Switch Loopback Test


          Number to Dial Directory Number 1: 5105776430
          Number to Dial Directory Number 2: 5105776431


                          Run Test Now


                          Status: Untested
```
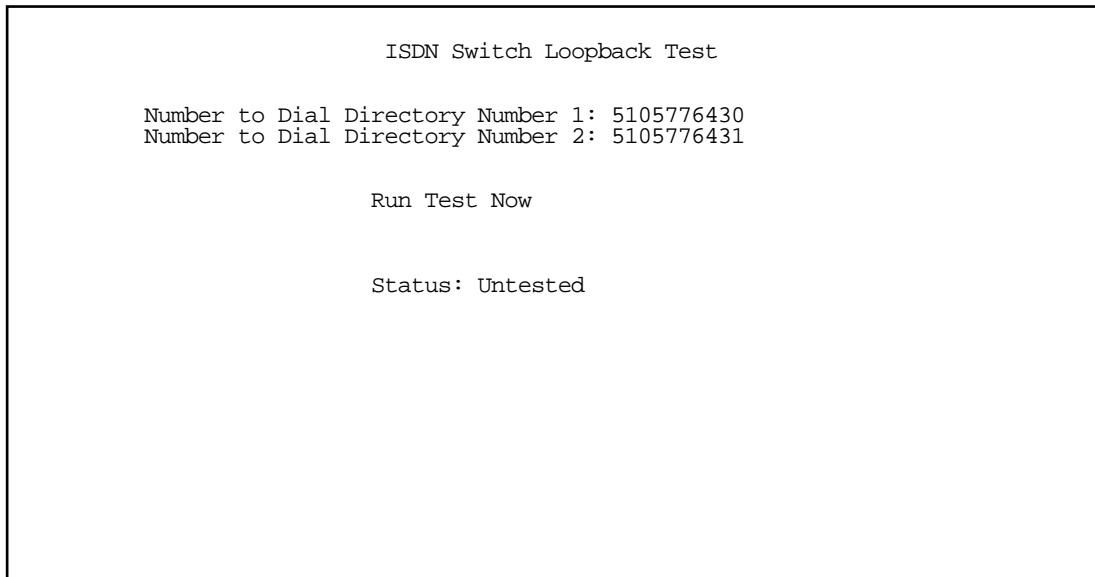
Note: "Number to Dial Directory Number 1 and 2" fields are only visible if there are no DNs in the ISDN line configuration.

Select **Run Test Now** and press Return. The loopback test is executed immediately.

Note: Make sure neither B-channel is in use before you execute the loopback test.

The **Status** item reports one of three results:

Untested: The loopback test has not yet been run.

Loopback Test FAILED: The loopback test has failed. See "If the loopback test fails," below, for troubleshooting suggestions.

Loopback Test PASSED. The loopback test was successful. The line is working properly, and the directory numbers (the ISDN phone numbers associated with each B-channel) are correct. If a SPID is associated with the first B-channel, its correctness is also confirmed. If a SPID is associated with the second B-channel, its correctness is confirmed. SPIDs are only applicable to certain North American ISDN switch protocols.

If the loopback test fails

Follow these suggestions to track down the reason behind the loopback test's failure:

■ Check that the WAN Ready LED is solid green.

■ Check the ISDN event log and get more information about events that seem relevant to the failure.

■ Check the B-channel usage in the Quick View screen to make sure there were no active calls when the loopback test was performed.

■ Check the accuracy of the directory numbers, SPIDs, and switch protocol you entered in the ISDN Line Configuration screen (compare them with the information you received from your ISDN service provider).

■ Verify termination of the S/T bus.

■ Contact your ISDN service provider to have the line checked.

■ Check that your line is not provisioned for voice only (Circuit Switched Voice).

Part III: Appendixes

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while setting up and using the Netopia R3100. It also includes information on how to contact Netopia Technical Support.

Important information on these problems may be found in the event histories kept by the Netopia R3100. These event histories can be accessed in the Statistics, Utilities, Tests screen.

This section covers the following topics:

■   "Configuration problems" on page A-1

■   "Power outages" on page A-3

■   "Technical support" on page A-3

Configuration problems

If you encounter problems during your initial configuration process, review the following suggestions before calling for technical support. There are four zones to consider when troubleshooting initial configuration:

1.   the computer's connection to the router;

2.   the router's connection to the telecommunication line(s);

3.   the telecommunication line's connection to your ISP, and

4.   the ISP's connection to the Internet.

If the connection from the computer to the router was not successful, check the following:

■   The Netopia R3100 is turned on.

■   An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Netopia R3100.

■   The SmartStart application is running and able to access the Netopia R3100.

■   Telnet is available on your PC or Macintosh. (On a PC, it must be specified in your system path. You can usually find the application as "c:\windowselnet.exe".)

■   Your PC or Macintosh has an IP address, either automatically or statically assigned, and compatible with the default IP address of the router, 198.162.1.1.

■   Your PC or Macintosh has a subnet mask that matches or is compatible with the Netopia R3100's default subnet mask, 255.255.255.0.

■   If you are entering a new IP address via SmartStart be sure the correct serial number was entered.

SmartStart Troubleshooting

The Status field of the SmartStart application will display information and indicate problems as they are detected.

Console connection problems

Can't see the configuration screens (nothing appears)

■   Check the cable connection from the Netopia R3100's console port to the computer being used as a console.

■   Check that the terminal emulation software is accessing the correct port on the computer that's being used as a console.

■   Try pressing Ctrl-L or Return or the ▲ up or down▼ key several times to refresh the terminal screen.

■   Check that flow control on serial connections is turned off.

Junk characters appear on the screen

■   Check that the terminal emulation software is configured correctly.

■   Check the baud rate. The default values are 9600, N, 8, and 1.

Characters are missing from some of the configuration screens

■   Try changing the Netopia R3100's default speed of 9600 bps and setting your terminal emulation software to match the new speed.

Network problems

This section contains tips on ways you can troubleshoot a networking problem.

Problems communicating with remote IP hosts

■   Verify the accuracy of the default gateway's IP address (entered in the IP Setup or Easy Setup screen).

■   Use the Netopia R3100's ping utility, in the Statistics, Tests, Utilities screen, and try to ping local and remote hosts. See "Ping" on page 16-2 for instructions on how to use the ping utility. If you can successfully ping hosts using their IP addresses but not their domain names (198.34.7.1 but not garcia.netopia.com, for example), verify that the DNS server's IP address is correct and that it is reachable from the Netopia R3100 (use ping).

■   If you are using filters, check that your filter sets are not blocking the type of connections you are trying to make.

Local routing problems

■   Observe the Ethernet LEDs to see if data traffic flow appears to be normal.

■   Check the WAN Statistics and LAN Statistics screens to see more specific information on data traffic flow and address serving.

Power outages

If you suspect that power was restored after a power outage, and the Netopia R3100 is connected to a remote site, you may need to switch the Netopia R3100 off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the router should reestablish the connection.

Technical support

Netopia, Inc. is committed to providing its customers with reliable products and documentation, backed by excellent technical support on-line and through our resellers and distributors.

Before contacting Netopia

Look in this guide for a solution to your problem. You may find a solution in this troubleshooting appendix or in other sections. Check the index for a reference to the topic of concern. If you cannot find a solution, complete the environment profile below before contacting technical support.

Environment profile

■   Locate the Netopia R3100's model number, product serial number, and firmware version. The serial number is on the bottom side of the Router, along with the model number. The firmware version appears in the Netopia R3100's Main Menu screen.

Model number:

Serial number:

Firmware version:

■   What kind of local network(s) do you have, with how many devices?

Ethernet

LocalTalk

EtherTalk

TCP/IP

IPX

Other:

How to get support

We can help you with your problem more effectively if you have completed the environment profile in the previous section. If you contact your local reseller or distributor by telephone, please be ready to supply them with the information you used to configure the Netopia R3100. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

You may also contact Netopia Technical Support directly by e-mail, telephone, fax, or post:

Internet: techsports@netopia.com (for technical support)
info@netopia.com (for general information)

Phone: 1 800-782-6449
Fax: 1 510-814-5023

Netopia, Inc.
Customer Service
2470 Mariner Square Loop
Alameda, California 94501
USA

Netopia Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Netopia World Wide Web server via http://www.netopia.com
Internet via anonymous FTP to ftp.netopia.com/pub

FAX-Back

This service provides technical notes which answer the most commonly asked questions, and offer solutions for many common problems encountered with Netopia products.

FAX-Back: +1 510-814-5040

Appendix B

Setting Up Telco Services

This chapter describes how to obtain telco services from your telephone service provider.

This section covers the following topics:

■   "Obtaining an ISDN line" on page B-1

■   "Completing the ISDN worksheet" on page B-5

North America only

Note: If you signed up for Netopia's Up & Running, Guaranteed! program, Netopia will set up an ISDN or leased line service with your telephone company, set up Internet services from your ISP, and configure your Netopia Router.

You may still want to read this chapter for information on how to obtain and set up telco services from your telephone service provider.

Obtaining an ISDN line

To obtain an ISDN line:

1.   Find an ISDN service provider — see below.

2.   Choose the type of ISDN line you need — see "Choosing an ISDN line" on page B-1

3.   Order the ISDN line — see "Ordering an ISDN line" on page B-1.

Note: Worksheets are provided on page B-6 and page B-7 to simplify the procedure for obtaining an ISDN line.

Finding an ISDN service provider

In North America, local telephone companies typically provide ISDN service. However, in certain regions, long-distance telephone companies or other vendors may provide ISDN service. If you are unsure of who provides ISDN service in your area, contact your local telephone company. For your convenience, Farallon provides a list of North American Internet service providers on its World Wide Web site: www.netopia.com.

Outside North America, local telephone companies typically provide ISDN service.

Choosing an ISDN line

■   Order an ISDN line that supports both data and voice. Some providers charge less for voice provisioning.

■   Order an IDSL (ISDN Digital Subscriber Line) for cost savings if you will use a Point to Point copper pair ("Dry Line") connection.

Ordering an ISDN line

The following sections provide items to consider when ordering an ISDN line.

The physical ISDN line

You can either convert an existing analog telephone line to ISDN or install a new ISDN line.

In either case, make sure there is a wall jack for the line near the location where you intend to install the Netopia Router.

In many cases, ISDN can use the same physical wire used for analog service. For more information consult with your ISDN service provider.

Note: You cannot connect analog equipment, such as telephones, facsimile machines, and modems directly into an ISDN line, without special equipment. If your Netopia Router supports SmartPhone™, you can attach analog telephony devices to the phone jacks on the back of the Netopia Router.

If your site has only one telephone line, or if you will be using a Netopia Router that does not support SmartPhone, we recommend you keep the existing analog line to conduct non-ISDN communications.

Setup tips

Your ISDN service provider may have the Netopia Router on a list of supported products that have been tested with a particular ISDN line configuration. Your ISDN service provider will know how to set up your line if the Netopia Router is on that list.

If your Netopia Router supports SmartPhone™, inform your ISDN service provider that you will have both voice and data services.

ISDN Ordering Codes

For North America, if your ISDN service provider is familiar with North American ISDN Users Forum (NAIUF) Capability Packages, you may request one of the following ISDN Ordering Codes (IOCs):

■ **Capability Package R** (2B) includes circuit-switched data on two B-channels. Data capabilities include Caller ID, but voice features are unsupported.

  This package can be used with a Netopia Router that does not have voice capabilities (does not support SmartPhone) and will never use data over voice speech-based calls. Models that could use this provisioning are the 440, 630, and 640.

■ **Capability Package S** (2B) includes alternate voice/circuit-switched data on two B-channels. Data and voice capabilities include Caller ID and Redirecting Number Delivery.

  This package can be used with Netopia Routers that support SmartPhone, but not Advanced Calling features like ACO. Models that include the SmartPhone services are the 435 and 635. This package can also be used for Netopia Routers without SmartPhone that would use just data over voice speech-based calls. Models that could support this feature are the 440, 630, and 640.

■ **Capability Package U** (2B), also known as EZ-ISDN1, includes alternate voice/circuit-switched data on two B-channels. Voice capabilities include non-EKTS (non-Electronic Key Telephone Service) voice features including Call Forwarding Variable, Additional Call Offering, Flexible Calling, and Caller ID, which includes Redirecting Number Delivery. Data capabilities include Caller ID which also provides Redirecting Number Delivery.

  This package is recommended for Netopia Routers that offer SmartPhone services. Models that could use this provisioning are the 435 and 635.

Note: Check with your telephone service provider for cost differences between the various IOCs listed above, when ordering or provisioning your ISDN line.

Not all telephone service providers are aware of IOCs. Even though these providers may not understand IOCs, they will be familiar with the features and parameters that the IOC defines and can provision the ISDN line accordingly.

For a complete listing of all IOCs, or for more information about IOCs, refer to the Bell Communications Research web site at 'www.bellcore.com'.

In addition, Appendix A contains a reference table summarizing the recommended provisioning parameters offered by various North American ISDN switches.

Switch protocol type

To configure the Netopia Router, your ISDN service provider must provide you with the switch protocol type used on your ISDN line.

Outside North America only

The Netopia Router supports the following protocols:

■   EuroISDN (also known as ETSI or NET3)

■   Japanese NTT

■   Australian TS013

North America only

The Netopia Router supports the following protocols:

■   An AT&T 5ESS, Northern Telecom DMS-100, or a Siemens EWSD running National ISDN-1 (NI-1)

■   AT&T 5ESS custom (multipoint or point-to-point)

■   Northern Telecom DMS-100 custom

■   IDSL (ISDN Digital Subscriber Line)

■   Ascend MP+

Directory and SPID numbers (U models only)

A North American ISDN line requires one or more directory numbers (DN) and usually one or more service profile identifier (SPID) numbers. Your ISDN service provider supplies this information when you order your ISDN line or after your ISDN line is set up. Once you obtain this information, record it on the worksheet (see page B-6).

Note: If the switch on your line is an AT&T 5ESS custom point-to-point or IDSL, you will receive no SPIDs, just a single DN.

Circuit ID number (U models only)

A North American ISDN line has a unique physical address called a circuit ID. You should obtain this number from your ISDN service provider and record it on the worksheet (see page B-6). The circuit number can help locate your line and its associated circuit in case of a problem.

Long-distance ISDN calls (North American models only)

If you are interested in placing long-distance calls on your Netopia Router, you will want to sign up with a long-distance telephone carrier company that offers connectivity over ISDN. When the Netopia Router places long-distance calls on your ISDN line, you will then be automatically billed by a long-distance telephone company. Therefore, make sure you use a long-distance company of your choice for your ISDN line.

Note: If you choose not to have a long-distance carrier, calls placed out of your local area will fail.

ISDN Service Provider information (North American models only)

If your ISDN service provider does not recognize the Netopia Router or ordering codes, provide them with the ISDN Provisioning information in Appendix A.

Testing the ISDN line

Once the Netopia Router is installed and configured, use the loopback test to evaluate the line. See "ISDN Switch Loopback Test" on page 16-13. If the line does not work properly, ask your ISDN service provider to reconfigure the line until it works properly. A successful loopback is necessary for a bonded 128K 2B connection.

Completing the ISDN worksheet

The following ISDN worksheets are provided for you to enter ISDN account information. For your convenience, you may want to photocopy the appropriate ISDN worksheet, and then complete the copy.

When completing the worksheet, fill in:

■   Section 1 when you find out from whom you'll be ordering your ISDN line.

■   Section 2 when ordering your ISDN line.

■   Section 3 after ordering your ISDN line.

Complete the worksheet carefully. You will need this information when configuring the Netopia Router.

Have the worksheet available if you call Farallon Technical Support. The information on the sheet will help a Farallon technician answer your questions quickly.

Note: The ISDN worksheet is for your convenience only. You may receive forms containing similar information from your ISDN service provider. The ISDN worksheet is neither an application for an ISDN line nor a substitute for the forms your ISDN service provider uses.

ISDN Telco Worksheet for North America

1. ISDN Service Provider (Telephone Company) contact information

Name and Address:

_____

_____

Telephone/Fax numbers:_____

E-mail address: _____

2. Your information

Street address where your ISDN line is located:

_____

_____

Contact person at this location, including phone number:

_____

Is this an existing line or a new line (to be installed)? __ existing __ new

List number in the telephone company's directory? __ no __ yes

Billing address for your ISDN line:

_____

_____

3. ISDN information

ISDN line configuration method used (check one):

__ By product (Netopia Router)   __ Other method

Type of switch (check one):

__ NI-1   __ AT&T 5ESS custom

__ Northern Telecom DMS-100 custom   __ IDSL

Primary directory number (ID 1): _____

Primary SPID (1): _____

Secondary directory number (ID 2):_____

Secondary SPID (2):_____

Circuit ID number:_____

Long-distance carrier used on ISDN line: _____

Type of services (check one)

 __ voice and data (B 1)   __ voice and data (B 2)   __ data only

ISDN Telco Worksheet for Outside North America

1. ISDN Service Provider (Telephone Company) contact information

Name and Address:

_____

_____

Telephone/Fax numbers: _____

E-mail address: _____

2. Your information

Street address where your ISDN line is located:

_____

_____

Contact person at this location, including phone number:

_____

Is this an existing line or a new line (to be installed)? __ existing __ new

List the number in the telephone company's directory? __ no __ yes

Billing address for your ISDN line:

_____

_____

3. ISDN information

ISDN line configuration method used (check one):

__ By product (Netopia Router)   __ Other method

Type of switch (check one):

__ EuroISDN (ETSI, NET3)

–– Japanese NTT

–– Australia TS013

Primary directory number (ID 1): _____

Secondary directory number (ID 2): _____

Type of services (check one)

__ voice and data (B 1)   __ voice and data (B 2)   __ data only

Appendix C

North American Telco Provisioning for ISDN

North American ISDN BRI

Provisioning Parameters	5ESS NI-1	5ESS Multipoint	5ESS Pt-to-Pt	DMS-100 NI-1	DMS-100 Custom
Protocol Version Control (PVC)	N/A			PVC-2	PVC-2
Terminal Type	Type-A			N/A	
TEI Assignment	Dynamic				
Directory Numbers	2		1	2	
CSD/CSV for DN1	Both				
CSD/CSV for DN2	Both		N/A	Both	
Packet on D/B (PSD/PSB)	No				
Circuit Switched Voice (CSV)	1			N/A	
Call Appearance				2	
Call Appearance Quality		2		N/A	
CSV Channel	Any			N/A	
CSV Additional Call Offering (ACO)	Unrestricted			Custom	Yes
CSV Limit	2			N/A	
CSV Notification Busy (NB) Limit	1			N/A	
Circuit Switched Data (CSD)	2			N/A	
CSD Channel	Any			N/A	
CSD Additional Call Offering (ACO)				N/A	
CSD Limit	2			N/A	
CSD Notification Busy (NB) Limit				N/A	
Additional Call Offering	N/A*			Yes	
Electronic Key System (EKTS)				No	
Maximum Keys	N/A			9 or 64	
Ringing	N/A			Yes	
Release Key	N/A			No	
Flexible Calling	No **				
Caller ID Delivery	Yes ***				

   * While not a 5ESS NI-1 parameter, this feature is supported.
     This feature is not available on 5ESS custom (Multipoint or Pt-to-Pt).

  ** Flexible Calling includes Hold, Drop, Conference, and Transfer.
     Future Netopia firmware releases will support these features.

 *** Caller ID Delivery may not be available from your ISDN provider.

Appendix D

Setting Up Internet Services

This chapter describes how to obtain and set up Internet Services.

This section covers the following topics:

- "Finding an Internet service provider" on page D-1
- "Deciding on an ISP account" on page D-2
- "Obtaining information from the ISP" on page D-3

Note: Some companies act as their own ISP. For example, some organizations have branch offices that can use the Netopia R3100 to access the Internet via the main office in a point-to-point scenario. If you install the Netopia R3100 in this type of environment, refer to the following sections for specific information you must receive from the network administrator to configure the Netopia R3100 properly.

Finding an Internet service provider

Internet access is available from Internet service providers (ISPs). Typically, there are several ISPs in each area. To locate ISPs in your area, consult your telephone book, local computer magazines, the business section of a local newspaper, or the following URL on the Internet: 'http://www.thelist.com'. Also see Netopia's home page at 'http://www.netopia.com' for a list of special programs and promotions for Netopia customers.

If your area has more than one ISP, the following considerations may help you decide which ISP is best suited for your requirements.

Use an ISP that provides Internet access through a digital line that supports the following:

Type of Service	Data Rate Speed	Datalink Protocol
ISDN	56/64-128 kbps	PPP, HDLC, Frame Relay

Unique requirements

Make sure the ISP can meet any unique requirements you may have. Potential requirements include:

- Dynamic or static IP addressing
- Class C IP address
- Custom domain name
- Multiple email addresses
- Web site hosting
- Call back for web site hosting at your site

Pricing and support

Compare pricing, service, and technical support service among various ISPs.

ISP's Point of presence

Check with your ISP for the location of their nearest point of presence (POP) in reference to your site. In some instances, the ISP that you choose may not offer a POP in your local area. If that is the case, you may incur additional fees for long-distance calls.

Endorsements

Consider recommendations from colleagues and reviews in publications. Netopia lists Netopia Certified ISPs on our web site at 'http://www.netopia.com'.

Deciding on an ISP account

Your ISP may offer various Internet access account plans. Typically, these plans vary by usage charges and the number of host IP addresses supplied. Evaluate your networking needs and discuss them with your ISP before deciding on a plan for your network.

The following checklist is a guide to ensure you obtain the Internet service you require.

Setting up a Netopia R3100 account

Check whether your ISP has the Netopia R3100 on a list of supported products that have been tested with a particular configuration. If the ISP does not have the Netopia R3100 on such a list, describe the Netopia R3100 in as much detail as needed, so your ISP account can be optimized. As appropriate, you may refer your ISP to Netopia's web site for more information.

Obtaining an IP host address

Typically, each computer on the network that requires Internet access requires its own unique IP address. If some or all network computers require simultaneous Internet access, obtain a block of IP host addresses large enough for each computer to have its own address, plus one for the Netopia R3100.

Consider expected growth in your network when deciding on the number of addresses to obtain. Alternatively, you may use the Network Address Translation feature of SmartIP.

SmartIP™

The Netopia R3100 ISDN Router supports the SmartIP™ feature which includes Network Address Translation.

Network Address Translation provides Internet access to the network connected to the Netopia R3100 using only a single IP address. These routers translate between the internal or local area network (LAN) addresses and a single external IP address and route accordingly.

For more information on Network Address Translation, see Chapter 11, "IP Setup and Network Address Translation."

Obtaining information from the ISP

After your account is set up, the ISP should send you the IP parameter information that will help you to configure the Netopia R3100.

Local LAN IP address information to obtain

With Network Address Translation

If you are using SmartIP (NAT), you should obtain the following:

■   If you are dialing out to a remote site using Network Address Translation on your router, your provider will not define the IP address information on your local LAN. You can define this information based on parameters defined by another connection profile such as that to a corporate network, or an IP configuration that may already be in place for the existing network. Alternatively, you can use the default IP address range used by the router.

■   Primary and Secondary Domain Name Server (DNS) IP Addresses

■   Domain Name (usually the same as the ISP's domain name unless you have registered for your own individual domain name)

Remote WAN IP address information to obtain

■   Telephone number of the ISP's local or nearby dial-up POP (point-of-presence).

■   PPP authentication type for router at the ISP, such as PAP.

■   Send and receive User Login name and Send and receive User Password if PAP or CHAP security authentication is used

Without Network Address Translation

If you are not using SmartIP (NAT), you should obtain:

■   The number of Ethernet IP host addresses available with your account and the first usable IP host address in the address block

■   The Ethernet IP address for your Netopia R3100

■   The Ethernet IP subnet mask address for your Netopia R3100

■   The Default Gateway IP Address (same as Remote IP Address in most cases)

■   Primary and Secondary Domain Name Server IP Addresses

■   Domain Name (usually the same as the ISP's domain name unless you have registered for your own individual domain name)

Note: If you are not using Network Address Translation, you will need to obtain all of the Local LAN IP address information from your ISP.

Remote WAN IP address information to obtain

■ The telephone number of the ISP's local or nearby dial-up POP (point-of-presence).

■ Remote IP address of router at ISP or other remote site

■ Remote IP subnet mask address of router at ISP or other remote site

■ PPP authentication type for router at the ISP, such as PAP.

■ Send User Login name and Send User Password if PAP or CHAP security authentication is used

Note: If you are not using Network Address Translation, you will need to obtain all of the Remote WAN IP address information from your ISP.

Appendix E

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia R3100 and using some of its powerful features, such as static routes and packet filtering.

In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

This section covers the following topics:

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate.

Note: This guide uses the term "IP" in a very general and inclusive way, to identify all of the following:

■   Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP

■   Packets that include an IP header within their structure

■   Devices that send IP packets

About IP addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts, instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.168.1.1 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations who request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1-127	127	16,777,214	net.host.host.host	97.3.14.250
B	128-191	16,384	65,534	net.net.host.host	140.100.10.11
C	192-223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP routers, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits, in order to leave room for the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses, and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation, like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network, when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP routers and gateways such as the Netopia R3100.

Note: If you receive a routed account from an ISP, there must be a mask associated with your network IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

When setting up IP routing with a Class A Address, or even multiple Class C Addresses, subnetting is fairly straightforward. Subnetting a single Class C address between two networks, however, is more complex. This section describes the general procedures for subnetting a single Class C network between two Netopia routers so that each can have Internet access.

Network configuration

Below is a diagram of a simple network configuration. The ISP is providing a Class C address to the customer site, and both networks A and B want to gain Internet access through this address. Netopia R3100 B connects to Netopia R3100 A and is provided Internet access through Routers A and B.

Customer Site A

PC 1:
IP Address: 192.168.1.3
Subnet Mask: 255.255.255.128
Gateway: 192.168.1.1

Router B:
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.128
Remote IP: 10.0.0.1
Remote Sub: 255.255.255.0
Gateway: 10.0.0.1
Static Route: 192.168.1.128 [network] 255.255.255.128 [mask] 192.168.1.2 [via router]
Usable IP Addresses available to Customer Site A: 192.168.1.1 --> 192.168.1.126

Netopia R3100 A:
IP Address: 192.168.1.2
Subnet Mask: 255.255.255.128
Remote IP: 192.168.1.129
Remote Sub: 255.255.255.128
Gateway: 192.168.1.1
Usable IP Addresses available to Customer Site A: 192.168.1.1 --> 192.168.1.126

LAN

ISP Network

Router A:
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0

Customer Site B

PC 2:
IP Address: 192.168.1.130
Subnet Mask: 255.255.255.128
Gateway: 192.168.1.129

Netopia R3100 B:
IP Address: 192.168.1.129
Subnet Mask: 255.255.255.128
Remote IP: 192.168.1.2
Remote Sub: 255.255.255.128
Gateway: 192.168.1.2
Usable IP Addresses available to Customer Site B: 192.168.1.129 --> 192.168.1.254

Internet

LAN

Background

The IP Addresses and routing configurations for the devices shown in the diagram are outlined below. In addition, each individual field and its meaning are described.

The "IP Address" and "Subnet Mask" fields define the IP Address and Subnet Mask of the device's Ethernet connection to the network while the "Remote IP" and "Remote Sub" fields describe the IP Address and Subnet mask of the remote router. This information is entered in the Connection Profile of the Netopia R3100.

The "Gateway" field describes the router or workstation's default gateway or, where they will send their packets if the appropriate route is not known. The "Static Route" field, which is only shown on Router B, tells Router B what path to take to get to the network defined by Netopia R3100 B. Finally, the "Usable IP Address" field shows the range of IP Addresses available to the hosts of that network.

Note that the IP Addresses given in this section are for example purposes only. Do not use these addresses when configuring your network.

With this configuration, both Customer Site A and B can gain Internet access through Routers A and B, with no reconfiguration of the ISP's equipment. The most important item in this configuration is the Static Route defined on Router B. This tells Router B what path to take to get to the network defined by Netopia R3100 B. Without this information, Customer Site B will be able to access Customer Site A, but not the Internet.

If it is not possible to define a Static Route on Router B, RIP could be enabled to serve the same purpose. To use RIP instead of a Static Route, enable Transmit RIP on Netopia R3100 A and Transmit and Receive RIP on Router B. This will allow the route from Customer Site B to propagate on Router B and Customer Site A.

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts, and no plans to add any new hosts. You don't need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you may obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP's network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages to this situation is the greater ease and lower cost of obtaining a subnet from an ISP rather than a full Class C address.

Distributing IP addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an Internet service provider. When configuring the Netopia R3100, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

There are two schemes for distributing the remaining IP addresses:

■ Manually give each computer an address

■ Let the Netopia R3100 automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Netopia R3100. Using the Router in this way allows it to function as an address server.

One reason to use the Netopia R3100 as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You only need to enter information once, rather than having to repeatedly enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Netopia R3100 as an address server is that it will only distribute addresses to hosts that need to use them.

All Netopia R3100s come with an integrated Dynamic Host Control Protocol (DHCP) server. Some routers also come with a Macintosh Internet Protocol (MacIP) server. These servers provide a means of distributing IP addresses to either a Mac or PC workstation as needed.

When setting up the DHCP or MacIP servers in the Netopia R3100, it is necessary to understand how workstations lease, renew, and release their IP addresses. This information will be helpful in determining dynamic address allocation for a network.

The term "lease" describes the action of a workstation requesting and using an IP address. The address is dynamic and can be returned to the address pool at a later time.

The term "renew" refers to what the workstations do to keep their leased IP address. At certain intervals, the workstation talks to the DHCP or MacIP server and renews the lease on that IP address. This renewal allows the workstation to keep and use the assigned IP address until the next renewal period.

The term "release" refers to a situation where the workstation is no longer using its assigned IP address or has been shut down. IP addresses can be manually released as well. The IP address goes back into the DHCP or MacIP address pool to be reassigned to another workstation as needed.

Technical note on subnet masking

Note: The IP address supplied by the Netopia R3100 will be a unique number. You may wish to replace this number with a number that your ISP supplies if you are configuring the router for a static IP address. The automatic IP mask supplied by SmartStart is a Class C address. However, the Netopia R3100 and all devices on the same local network must have the same subnet mask. If you require a different class address, you may edit the IP Mask field to enter the correct address. Refer to the table below.

Number of Devices (other than Netopia R3100) on Local Network	Largest Possible Ethernet Subnet Mask
1	255.255.255.252
2-5	255.255.255.248
6-13	255.255.255.240
14-29	255.255.255.224

Number of Devices (other than Netopia R3100) on Local Network	Largest Possible Ethernet Subnet Mask
30-61	255.255.255.192
62-125	255.255.255.128
125-259	255.255.255.0

Configuration

This section describes the specific IP address lease, renew, and release mechanisms for both the Mac and PC, with either DHCP or MacIP address serving.

DHCP Address Serving

Windows 95 Workstation:

■ The Win95 workstation requests and renews its lease every half hour.

■ The Win95 workstation does NOT relinquish its DHCP address lease when the machine is shut down.

■ The lease can be manually expired using the WINIPCFG program from the Win95 machine, which is a command line program executable from the DOS prompt or from the START:RUN menu.

Windows 3.1 Workstation (MSTCP Version 3.11a):

■ The Win3.1 workstation requests and renews its lease every half hour.

■ The Win3.1 workstation does NOT relinquish its DHCP address lease when the user exits Windows and goes to DOS.

■ The lease can be manually expired by typing IPCONFIG /RELEASE from a DOS window within Windows or from the DOS prompt.</UL>

Macintosh Workstation (Open Transport Version 1.1 or later):

■ The Mac workstation requests and renews its lease every half hour.

■ The Mac workstation will relinquish its address upon shutdown in all but one case. If the TCP/IP control panel is set to initialize at start-up, and no IP services are used or the TCP/IP control panel is not opened, the DHCP address will NOT be relinquished upon shutdown. However, if the TCP/IP control panel is opened, or if an IP application is used, the Mac WILL relinquish the lease upon shutdown.

■ If the TCP/IP control panel is set to acquire an address only when needed (therefore a TCP/IP application must have been launched to obtain a lease) the Mac WILL relinquish its lease upon shutdown every time.

Netopia R3100 DHCP Server Characteristics

■ The Netopia R3100 ignores any lease-time associated with a DHCP request and automatically issues the DHCP address lease for one hour.

■ The Netopia R3100 does release the DHCP address back to the available DHCP address pool precisely one hour after the last heard lease request as some other DHCP implementations may hold on to the lease for an additional time after the lease expired, to act as a buffer for variances in clocks between the client

and server.

Macintosh Workstation (MacTCP or Open Transport):

Once the Mac workstation requests and receives a valid address, the Netopia R3100 will actively check for the workstation's existence once every minute.

■   For a DYNAMIC address, the Netopia R3100 will release the address back to the address pool after it has lost contact with the Mac workstation for over 2 minutes.

■   For a STATIC address, the Netopia R3100 will release the address back to the address pool after it has lost contact with the Mac workstation for over 20 minutes.

Netopia R3100 MacIP Server Characteristics

The Mac workstation uses ATP to both request and receive an address from the Netopia R3100's MacIP server. Once acquired, NBP confirm packets will be sent out every minute from the Netopia R3100 to the Mac workstation.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer's address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That's why manually distributed addresses are sometimes called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. A network administrator's computer, a computer dedicated to communicating with the Internet, and routers are appropriate candidates for a static address.

Using address serving

The Netopia R3100 provides two ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers.

The Netopia R3100 can use both DHCP and MacIP. Whether you use one or both will depend on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you will need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Tips and rules for distributing IP addresses

■   Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static addresses.

■   Note any planned and currently used static addresses before you use DHCP and MacIP.

■   Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

1   Distributed to the Netopia R3100
(Ethernet IP address)

2
3   Manually distributed
4   (static)

5
6
7
8
9
10   Pool of Addresses Distributed
11   by MacIP and DHCP
12
13
14
15
16

Block of IP host addresses
(derived from network IP
address + mask issued by ISP)
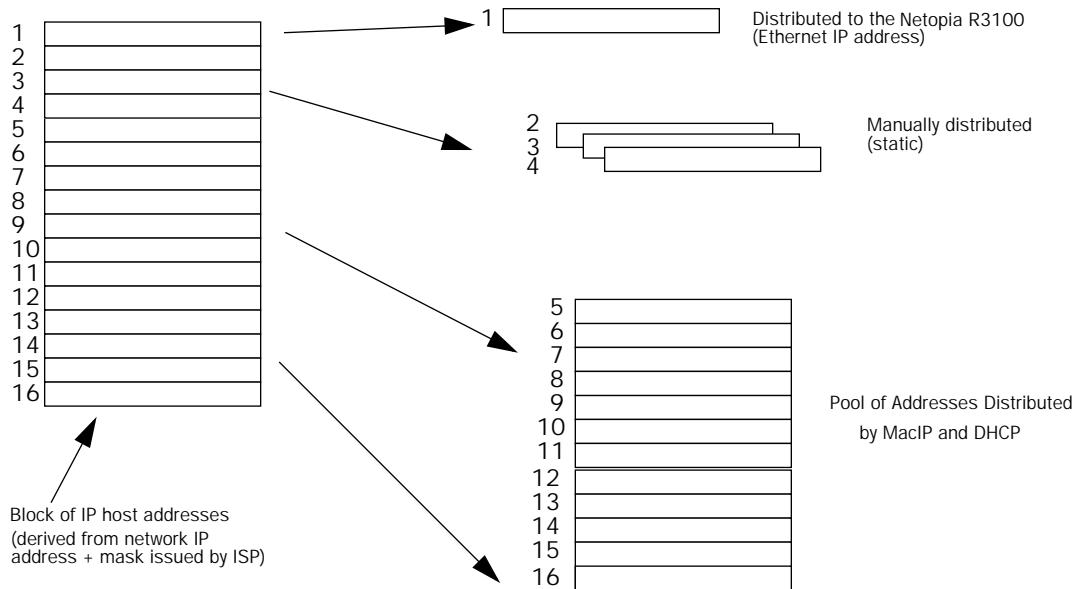
The figure above shows an example of a block of IP addresses being distributed correctly.

The example follows these rules:

■ An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.

■ A single IP address range is used by all the address-served clients. These include DHCP, BOOTP, MacIP, and WAN clients, even though BOOTP and static MacIP clients might not be considered served.

■ The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.

■ The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32, and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter "10" in the DHCP Setup screen's **Number of Addresses to Allocate** item. Then, in the same screen's **First Address** item, enter the first address in the sub-block to allocate such that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51).

Nested IP subnets

Under certain situations, you may wish to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses available to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

The figure at left shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Netopia R3100), a Netopia R3100, and a number of other hosts. Router A maintains a link to the Internet, and may be used as the default gateway.
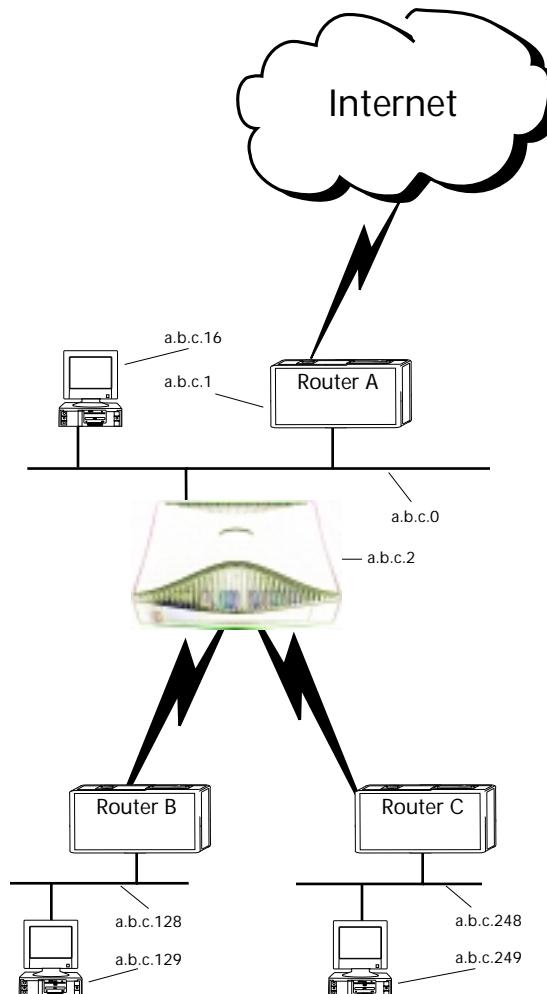
Routers B and C (which could also be Netopia R3100s) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Netopia R3100 with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
for Router B	a.b.c.128	255.255.255.192	7
for Router C	a.b.c.248	255.255.255.248	3

The Netopia R3100's connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:

```
                            IP Routing Table

     Network Address-Subnet Mask-----via Router------Port--Age--------Type------
     -------------------------------SCROLL UP-----------------------------------
     0.0.0.0           0.0.0.0         a.b.c.1 WAN     3719           Management
     127.0.0.1         255.255.255.255 127.0.0.1 lp1   6423           Local
     a.b.c.128         255.255.255.192 a.b.c.128 WAN   5157           Local
     a.b.c.248         255.255.255.248 a.b.c.248 WAN   6205           Local


     -------------------------------SCROLL DOWN---------------------------------
     UPDATE
```

Let's see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Netopia R3100, which examines its destination IP address.

The Netopia R3100 compares the packet's destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there's a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route's subnet mask, it yields a.b.c.248, which matches the network address in the route. The Netopia R3100 uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.

1 ────────────────

Address range available to a.b.c.0, less the two nested subnets

valid addresses used
by a.b.c.128

129

190

valid addresses used
by a.b.c.248

249

254
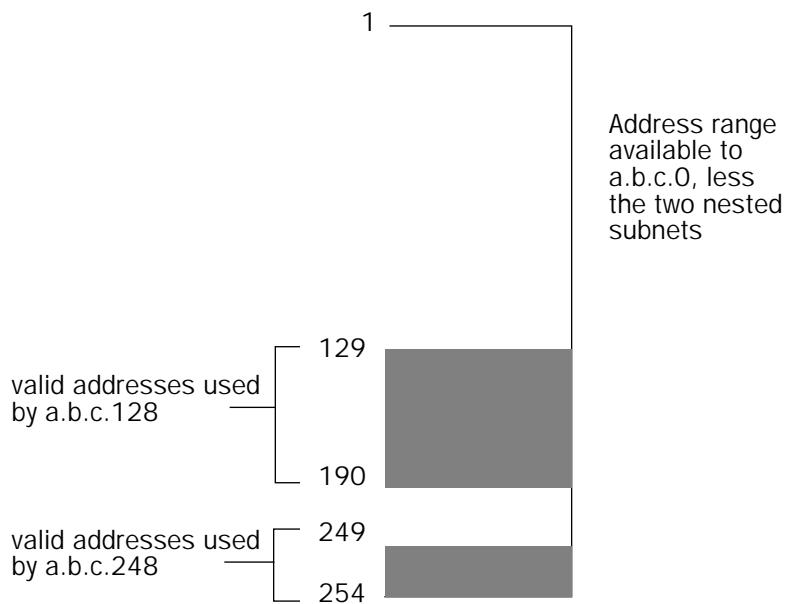
Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network, if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork, if the host address is all ones or all zeros but the subnet address is a combination or zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. By default, the Netopia R3100 uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

Appendix F

Understanding Netopia NAT Behavior

This appendix describes how Network Address Translation works within the Netopia R3100. The Netopia R3100 implements a powerful feature called Network Address Translation (NAT) as specified in RFC 1631. NAT is used for IP address conservation and for security purposes since there will only be a single IP "presence" on the WAN. This appendix describes the NAT functionality within the Netopia R3100 and provides examples for setup and use.

Network Configuration

Below is a diagram of the network referenced in this appendix.
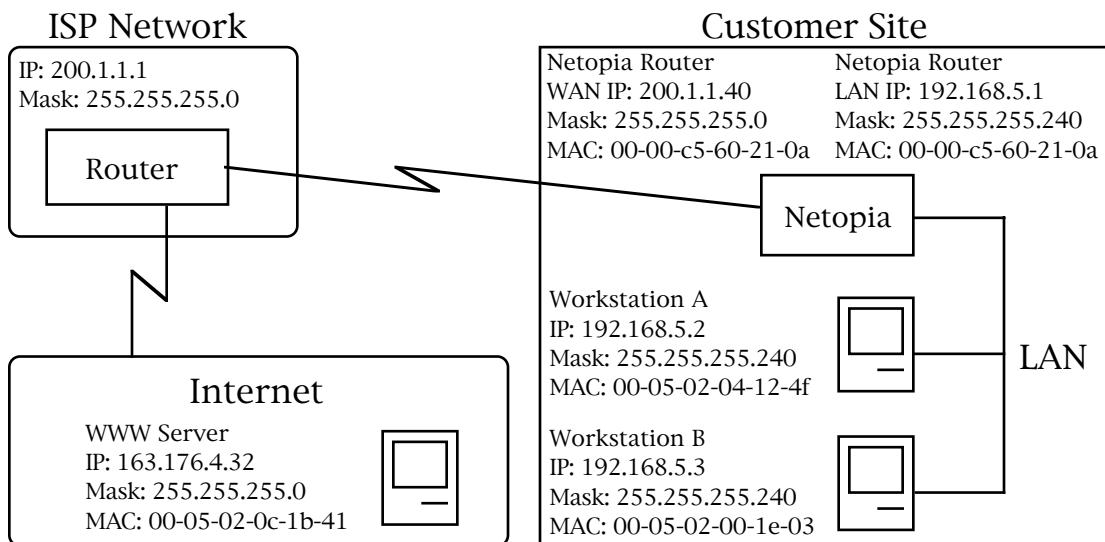
Background

NAT is a mechanism employed within the Netopia R3100 to acquire a statically or dynamically assigned IP address on its WAN interface and proxy against locally assigned IP addresses on its LAN interface. The Netopia R3100 uses a one-to-many IP address mapping scheme, that is against a single IP address the Netopia R3100 acquires on its WAN interface the Netopia R3100 can proxy 14, 30, or an unlimited number of IP hosts on the LAN interface.

In order to fully understand how NAT works you must understand how a PPP connection is established and IP addresses are negotiated.

When the Netopia R3100 establishes a connection over its WAN interface with another router it uses the Point to Point Protocol (PPP). Within PPP there is a Network Control Protocol (NCP) called Internet Protocol Control Protocol (IPCP) which handles the negotiation of IP addresses between the two routers, in this case the Netopia R3100 at the customer site above and the Router at the Internet Service Provider (ISP).

If the Netopia R3100 calls the Router at the ISP with NAT disabled, the Netopia negotiates its LAN interface address (as specified in IP Setup within the Netopia R3100's console) with the Router at the ISP through IPCP and then sets up routing. From the previous diagram you can see that the address for the Netopia R3100 is 192.168.5.1 and the address of the Router at the ISP is 200.1.1.1. Assuming that the addresses negotiated by the routers are valid and unique for the Internet, the Netopia R3100 and the hosts on its LAN would be able to access the Internet.

If the Netopia R3100 calls the Router at the ISP with NAT enabled, instead of negotiating the LAN interface address the Netopia R3100 suggests the address 0.0.0.0 through IPCP. When the Router at the ISP sees this all-zeros IPCP request, the Router can either pull a free dynamic IP address from its pool and assign it to the Netopia R3100's WAN interface or, if configured to do so, match the Netopia R3100's incoming connection profile and assign a pre-configured static IP address to the Netopia R3100's WAN interface.

From the previous diagram, you can see that the IP address assigned to the Netopia R3100's WAN interface is 200.1.1.40, while the IP address assigned to the LAN interface remains the same. The LAN interface address 192.168.5.1 is thus hidden from the ISP and the Internet, and the Netopia R3100 only has a single valid IP presence on the Internet. The LAN interface IP address for the Netopia R3100 can be any IP address, however it is recommended that you use the IANA specified 192.168.X.X Class C address range which is used for networks not attached to the Internet. This address range is described in RFC 1597.

The dynamic IP address acquisition on the WAN interface of the Netopia R3100 is one of several features of NAT. Another is the mapping of locally assigned IP addresses to the single globally unique IP address acquired by the Netopia R3100 on its WAN interface. NAT employs several things to accomplish this seamlessly. You must look at the formatting of an IP packet before IP address remapping can be explained.

Every IP packet that is transmitted across the Netopia R3100's LAN interface or across the WAN interface to the Internet contains several bits of information that indicate to any device where the packet is going and where it came from. In particular you have the source and destination port and source and destination IP addresses.

A port is used within IP to define a particular type of service and could be either a Transmission Control Protocol (TCP) port or User Datagram Protocol (UDP) port. Both TCP and UDP are protocols that use IP as the underlying transport mechanism. The major difference between TCP and UDP is that TCP is a reliable delivery service whereas UDP is a "best effort" delivery service. A list of well known TCP or UDP ports and services can be found in RFC 1700.

If Workstation A wants to communicate with a World Wide Web (WWW) Server on the Internet and the Netopia R3100 does not have NAT enabled, Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32. The source port could be 400 while the destination port would be 80 (WWW server). The Netopia R3100 then looks at this IP packet, determines the best routing method and sends that packet on its way across the WAN interface to the WWW Server on the Internet.

With NAT enabled the Netopia R3100 does something different. For example, suppose that Workstation A again wants to communicate with the WWW Server on the Internet. Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32 and source port could be 400 while the destination port would be 80 (WWW server).

When the Netopia R3100 receives this IP packet, it can not simply forward it to the WAN interface and the Internet since the IP addresses on the LAN interface are not valid or globally unique for the Internet. Instead the Netopia R3100 has to change the IP packet to reflect the IP address that was acquired on the WAN interface from the ISP.

The Netopia R3100 will first substitute the source IP address with the IP address that was acquired on the WAN interface which in this case is 200.1.1.40. Next the Netopia R3100 will substitute the source TCP or UDP port with a TCP or UDP port from within a specified range maintained within the Netopia R3100. And finally the modified IP packet's checksum is recalculated (as specified in RFC 1631) and the packet is transmitted across the WAN interface to its destination, the WWW Server on the Internet.

If the send and response IP packets were drawn out, this process would look like the following:
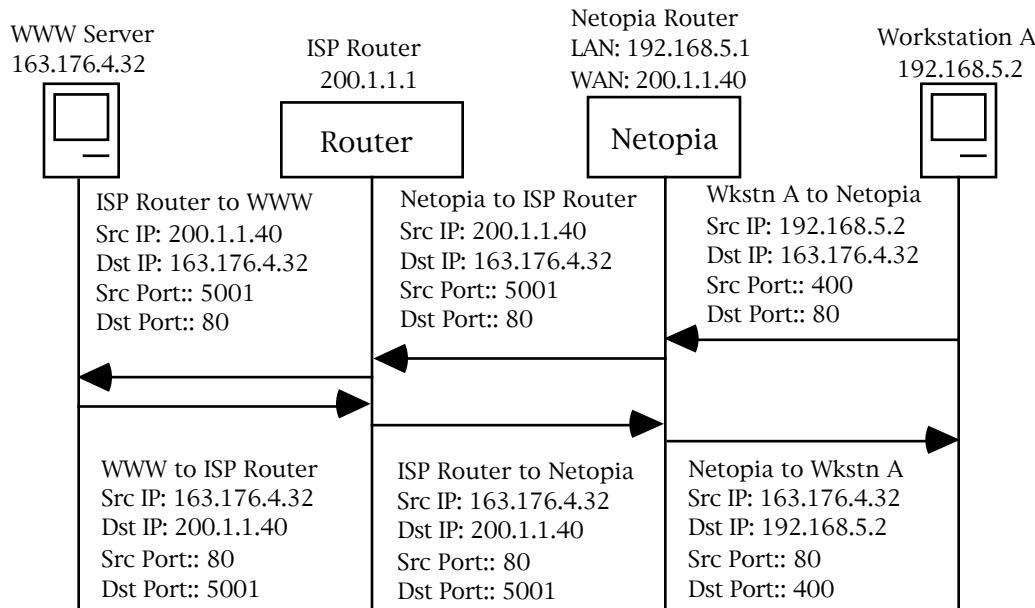
As you can see, the IP packet from Workstation A is sent to the Netopia R3100 and the source IP address is substituted with 200.1.1.40 and the source port is substituted with 5001, then the IP packet checksum is recalculated. When this modified packet reaches the WWW Server on the Internet, the WWW Server responds and sends the IP packet back to destination IP address 200.1.1.40 and destination port 5001.

When the Netopia R3100 receives this IP packet from the WWW Server, the Netopia R3100 replaces the destination IP address with 192.168.5.2, the address for Workstation A. The port is changed back to 400, the IP packet checksum is recalculated, and the IP packet is sent to Workstation A on the Netopia R3100s LAN interface.

The reasons for the IP address changes are obvious from the diagram above but what is not so obvious is why the TCP or UDP source ports need to be changed as well. These are changed and maintained in an internal table so the Netopia R3100 can determine which host on the local LAN interface sent the IP packet and what host the response from the WAN interface is going to go to on the LAN interface. This becomes especially important when two or more hosts on the LAN interface are accessing the same type of service on the Internet, like a WWW Server (Port 80), for example.

Now look at how two hosts on the LAN interface accessing the same WWW Server on the Internet will work:

WWW Server 163.176.4.32	ISP Router 200.1.1.1	Netopia Router LAN: 192.168.5.1 WAN: 200.1.1.40	Workstations A & B
	Router	Netopia	

ISP Router to WWW
Src IP: 200.1.1.40
Dst IP: 163.176.4.32
Src Port:: 5001
Dst Port:: 80

Netopia to ISP Router
Src IP: 200.1.1.40
Dst IP: 163.176.4.32
Src Port:: 5001
Dst Port:: 80

Wkstn A to Netopia
Src IP: 192.168.5.2
Dst IP: 163.176.4.32
Src Port:: 400
Dst Port:: 80

ISP Router to WWW
Src IP: 200.1.1.40
Dst IP: 163.176.4.32
Src Port:: 5002
Dst Port:: 80

Netopia to ISP Router
Src IP: 200.1.1.40
Dst IP: 163.176.4.32
Src Port:: 5002
Dst Port:: 80

Wkstn B to Netopia
Src IP: 192.168.5.3
Dst IP: 163.176.4.32
Src Port:: 400
Dst Port:: 80

WWW to ISP Router
Src IP: 163.176.4.32
Dst IP: 200.1.1.40
Src Port:: 80
Dst Port:: 5002

ISP Router to Netopia
Src IP: 163.176.4.32
Dst IP: 200.1.1.40
Src Port:: 80
Dst Port:: 5002

Netopia to Wkstn B
Src IP: 163.176.4.32
Dst IP: 192.168.5.3
Src Port:: 80
Dst Port:: 400

WWW to ISP Router
Src IP: 163.176.4.32
Dst IP: 200.1.1.40
Src Port:: 80
Dst Port:: 5001

ISP Router to Netopia
Src IP: 163.176.4.32
Dst IP: 200.1.1.40
Src Port:: 80
Dst Port:: 5001

Netopia to Wkstn A
Src IP: 163.176.4.32
Dst IP: 192.168.5.2
Src Port:: 80
Dst Port:: 400

As you can see, when Workstation A and Workstation B transmit an IP packet to the WWW Server on the Internet, they have unique source IP addresses on the LAN interface but potentially the same source ports, which in this case is 400. When the Netopia R3100 receives these packets, the source IP addresses are substituted with the single globally unique IP address that was acquired on the WAN interface which is 200.1.1.40.

Now both IP packets have the exact same source IP address (200.1.1.40) and source ports (400). The way the Netopia R3100 is then able to distinguish between the two IP packets is to change the source TCP or UDP ports and keep this information in an internal table. As seen above, the source port for Workstation A has been changed to 5001 and the source port for Workstation B has been changed to 5002.

If you were to look at the internal port mapping table that is maintained by the Netopia R3100, it would look similar to the following:

```
Source LAN IP     Source LAN Port     Remapped LAN Port
192.168.5.2       TCP 400             TCP 5001
192.168.5.3       TCP 400             TCP 5002
```

With this information the Netopia R3100 can determine the appropriate routing for an IP response from the Internet. In this case when the WWW Server responds with a destination port of 5001, the Netopia R3100 can see that this packet's destination on the local LAN interface is actually Workstation A at IP address 192.168.5.2. Likewise with the response for port 5002, the Netopia R3100 can see that this packet's destination on the local LAN interface is actually Workstation B at IP address 192.168.5.3.

Exported services

Note that this "automatic" port remapping and IP address substitution only works in one direction, for IP packets that originated on the LAN interface destined to the WAN interface and the Internet. In order for port remapping and IP address substitution to work in the other direction, that is, hosts on the Internet wishing to originate an IP packet destined to a host on the Netopia R3100s LAN interface, a manual redirection of TCP or UDP ports as well as destination IP addresses within the Netopia R3100 is required. This manual port remapping and IP address substitution is accomplished by setting up Exported Services.

Exported Services are essentially user defined pointers for a particular type of incoming TCP or UDP service from the WAN interface to a host on the local LAN interface. This is necessary since the Netopia R3100 and thus the attached local LAN has only one IP presence on the WAN interface and Internet. Exported Services allows the user to redirect one type of service, for example Port 21 (FTP), to a single host on the local LAN interface. This will then allow the Netopia R3100 to redirect any packets coming in from the Internet with the defined destination TCP or UDP port of Port 21 (FTP) to be redirected to a host on the local LAN interface.

For example, suppose the WWW Server on the Internet with the IP address of 163.176.4.32 wants to access Workstation B on the Netopia R3100s local LAN interface which is operating as an FTP Server. The IP address for Workstation B is 192.168.5.3, which is not a valid IP address and thus the WWW Server on the Internet can not use this IP address to access Workstation B.

The WWW Server on the Internet would then have to use the single valid IP address that was acquired on the Netopia R3100's WAN interface to access any host on the Netopia R3100's local LAN interface, since this is the only valid address for the Internet. But if the WWW Server on the Internet opens a connection to 200.1.1.40 via Port 21 (FTP) and no Exported Services are defined on the Netopia R3100, the Netopia R3100 will discard the incoming packet since the Netopia R3100 itself does not perform the requested service.

Thus you can see why Exported Services are necessary. In the example above, an Exported Service needs to be defined within the Netopia R3100 redirecting any incoming IP traffic with a destination port of 21 to the host on the local LAN interface with the IP address of 192.168.5.3.

If the WWW Server on the Internet then tries to open a connection to the IP address of 200.1.1.40 with the appropriate Exported Service defined, the Netopia R3100 will look at the destination port and will find that it is destined for Port 21 (FTP). The Netopia R3100 then looks at the internal user-defined Exported Services table and finds that any incoming IP traffic from the WAN port with a destination of Port 21 (FTP) should be redirected to the IP address of 192.168.5.3 on the local LAN interface, which in this case is Workstation B.

Once the appropriate Exported Services are defined, there can be seamless communication between a host on the Internet and a host on the Netopia R3100's local LAN interface.

Important notes

Even with the advantages of NAT, there are several things you should note carefully:

- There is no formally agreed upon method among router vendors to handle an all-zeros IPCP request. The majority of router vendors use the all-zeros IPCP request to determine when a dial-in host wants to be assigned an IP address. Some vendors however attempt to negotiate and establish routing with an all-zeros IP address. The Netopia R3100 will not allow routing to be established with an all-zeros IP address and the call will be dropped with an error logged in the Device Event History.

- When using NAT it is most likely that the Netopia R3100 will be receiving an IP address from a "pool" of dynamic IP addresses at the ISP. This means that the Netopia R3100's IP presence on the Internet will change with each connection. This can potentially cause problems with devices on the Internet attempting to access services like WWW and FTP servers or AURP partners on the Netopia R3100's local LAN interface. In this case, if a dynamic IP address is assigned to the WAN interface of the Netopia R3100 each time, the administrator of the Netopia R3100 will have to notify clients wishing to access services on the Netopia R3100's LAN interface of the new IP address after each connection.

- With NAT enabled, there cannot be two or more of the same types of service accessible from the Internet on the LAN interface of the Netopia R3100. For example, there cannot be multiple FTP servers (Port 23) on the Netopia R3100's LAN interface that can be accessible by workstations on the Internet. This is due to the fact that within the Netopia R3100 and IP there is no way to distinguish between multiple servers using the same port, in this case port 23.

- Fictional IP addresses may be assigned on the Netopia R3100's LAN interface. It is strongly recommended that for the Netopia R3100's LAN interface, an IP address from the Class C address range of 192.168.X.X be used. This is because this range is defined by the IANA as an address space that will never be routed through the Internet and is to be used by private Intranets not attached to the Internet.

  If the address range of 192.168.X.X is not used and another range of addresses such as 100.1.1.X is used instead, this address space can potentially overlap an address space that is owned by a user attached to the Internet. Thus if a user on the Netopia R3100's LAN interface has an IP address of 100.1.1.2 while the Netopia R3100's LAN interface is 100.1.1.2 and the local host wishes to access a host on the Internet with the address of 100.1.1.8, the Netopia R3100 has no way of knowing that the 200.1.1.8 address is actually on the Internet and not on its local LAN interface, as the local LAN interface is assigned the IP address range of 200.1.1.1 to 200.1.1.14.

Configuration

Network Address Translation is enabled by default with the SmartStart configuration utility. You can toggle **Enable Address Translation** to NO or YES in the Connection Profile screen in System Configuration under the IP Profile Parameters section. NAT is enabled on a per-profile basis, so it is possible to have any combination of NAT and non-NAT profiles. An example of enabling NAT is as follows:

```
                         IP Profile Parameters


         Remote IP Address:                  127.0.0.2
         Remote IP Mask:                     255.255.255.0

         Address Translation Enabled:        Yes

         Filter Set...
         Remove Filter Set

         Receive RIP:                        No






    Enter the remote IP network's IP address (form xxx.xxx.xxx.xxx decimal).
    Configure IP requirements for a remote network connection here.
```

Toggling Address Translation Enabled to Yes enables the Netopia R3100 to send out an all-zeros IPCP address that requests an IP to be assigned to the Netopia R3100's WAN interface. Note that the remote IP address is 127.0.0.2, which should also be the Default Gateway under IP Setup in System Configuration. This is done for profile matching purposes and because the IP address of the router the Netopia R3100 is dialing is not always known.

As mentioned earlier in this appendix, NAT works well for IP sessions originated on the Netopia R3100's LAN interface destined for the Internet without any additional configuration. For incoming IP connections from the Internet to a host on the Netopia R3100's LAN interface, Exported Services need to be used.

Exported Services are configured under IP Setup in System Configuration. This is where a particular type of TCP or UDP service originating from the Internet is redirected to a host on the Netopia R3100's LAN interface. An example of this screen is as follows:

```
                        Add Exported Service
                               +-Type------Port--+
                               +-----------------+
        Service...             | ftp        21   |
                               | telnet     23   |
                               | smtp       25   |
        Local Server's IP Address: | tftp   69   |
                               | gopher     70   |
                               | finger     79   |
                               | www-http   80   |
                               | pop2       109  |
                               | pop3       110  |
                               | snmp       161  |
                               | timbuktu   407  |
                               | pptp       1723 |
                               | irc        6667 |
                               | Other...        |
                               +-----------------+


          ADD EXPORT NOW                      CANCEL
```
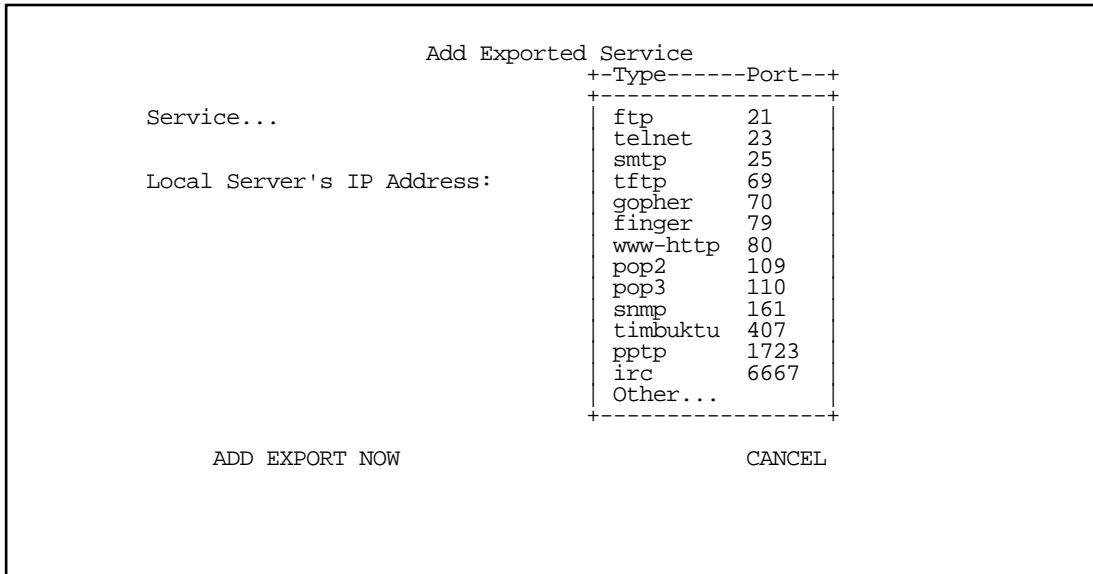
Within Exported Services is a pop-up containing a list of well known TCP and UDP services that can be redirected to a single host on the Netopia R3100's LAN interface. There is also an "Other…" option which allows for manual configuration of additional TCP or UDP ports. There can be a total of 32 Exported Services that can be defined.

When a particular type of service is redirected to an IP address, that service is removed from the pop-up list, since only one type of service can be redirected to a single host. However several different types of services can be redirected to a single or multiple hosts. For example, port 80 (WWW Server) could be redirected to 192.168.5.3 on the Netopia R3100's LAN interface as well as port 23 (Telnet) can be redirected to that same host.

Summary

NAT is a powerful feature of the Netopia R3100 and when used and set up properly can yield a secure network while only using one IP address on the WAN interface. Note that the addresses listed in this appendix are for demonstration purposes only. Do not use these addresses when configuring your local network.

Appendix G

Understanding Frame Relay

This appendix explains some of the major components of Frame Relay.

Frame Relay is a streamlined subset of the X.25 packet switching protocol which has been used by many corporations for wide area communications for a number of years. By removing the X.25 protocol error correction function and its associated overhead, Frame Relay can be used effectively up to T3 speeds over error-free lines (about 45 megabits per second).

The advantage provided by Frame Relay is its ability to combine multiple streams of "bursty" data (such as LAN protocol traffic) with relatively low average usage rates into a single channel with a relatively higher average usage rate. This "statistical multiplexing" effect allows your Frame Relay carrier to provide high bandwidth wide area connectivity to you at a price that is often significantly lower than standard leased line rates.

This section covers the following topics:

Virtual Circuits

Like X.25, Frame Relay is a connection-oriented service requiring your carrier to configure circuits to establish a physical link between two or more locations. A single, physical connection can support multiple virtual circuits (which appear as virtual point-to-point links).

There are two types of Frame Relay virtual circuits: Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs).

A PVC is a permanent association between two Frame Relay devices attached on a Frame Relay network. Once a PVC is defined, it requires no setup or disconnection. Each PVC has its own committed information rate, committed burst size, and excess burst.

SVCs are analogous to X.25 or ISDN connections, which require call setup and tear down.

Note: SVCs are generally not yet available from Frame Relay carriers. Virtually all Frame Relay communications presently use PVCs.

Committed Information Rate (CIR)

The Committed Information Rate is a tool your Frame Relay service provider uses to manage your PVCs. The CIR measures the average amount of normal priority data your Frame Relay network will attempt to deliver in a given time interval.

Committed Burst Size (B$_c$)

The Committed Burst specifies the maximum amount of data that your Frame Relay service provider agrees to transfer under normal conditions over the time interval T_c. The value for T_c is calculated with the formula:

$T_c = B_c / CIR$

Data in excess of B$_c$ may be discarded if the network becomes congested.

Excess Burst Size (B$_e$)

The Excess Burst specifies the maximum amount of data that your Frame Relay service provider will attempt to deliver over the time interval T_c.

In the absence of congestion, data will be transmitted at a rate equal to or less than the excess burst. That rate is calculated according to the following formula:

$(1 + B_e / B_c) * CIR$ = excess rate

Your Frame Relay service provider will attempt to deliver data containing excess bursts, but reserves the right to discard excess bursts in order to manage congestion within the network.
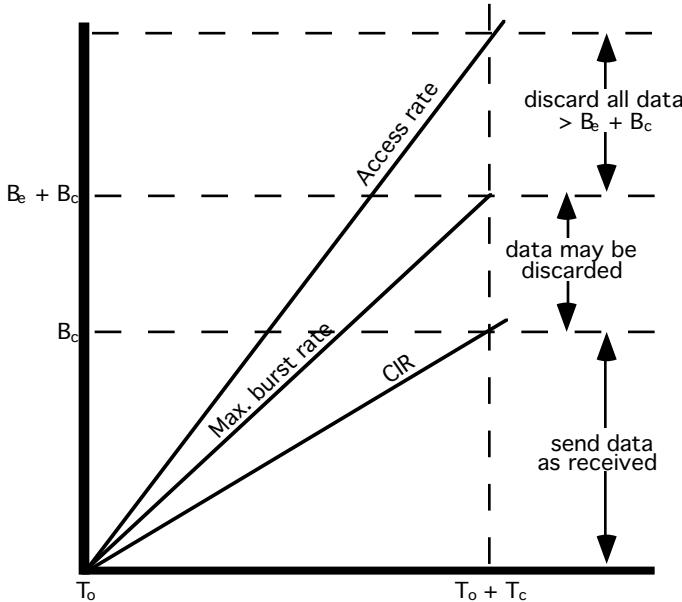
Actions of a Frame Relay Network

where:

B_c = Committed burst
B_e = Excess burst
CIR = Committed information rate
T_o = Beginning of interval
T_c = Interval B_c/CIR

Addressing

The logical address of a PVC is called the data link connection identifier (DLCI). The DLCI identifies each PVC within a shared physical channel.

Frame Relay packets are exchanged between nodes by mapping packets containing the source node's DLCI address to the destination DLCI address at the switch. Each switch contains a table identifying the various DLCIs with their associated user lines and interface trunks. However, the switch has more or less work depending on whether the DLCI has global or local significance.

Local and Global DLCIs

Local DLCI addressing means a Frame Relay virtual circuit (VC) will be identified by different DLCIs at each end. Frame Relay switches map across a VC, translating the "source" DLCI in a packet to the "destination" DLCI when forwarding the packet.

Global DLCI addressing is a Local Management Interface (LMI) extension that means a DLCI number identifies the same VC at both ends. Global addressing simplifies address administration but allows for only 1024 DLCIs in the entire network. The Frame Relay switch is not required to translate the DLCI in a packet as it does with local DLCIs.

Note: The majority of Frame Relay connections use Local DLCI addressing.

Local Management Interface (LMI)

The local management interface specifies communication between different Frame Relay devices (e.g., frame relay switches, routers, or access devices). Three local management interface specifications have been developed for Frame Relay:

■   The LMI consortium specification formulated by Cisco, DEC, Stratacom and Northern Telecom.

■   CCITT (Annex A)

■   ANSI (Annex D)

Note: The CCITT and ANSI specifications are formal outgrowths of the consortium LMI specification.

The Annex D specification is the most widely used in North America, although consortium LMI is still in use by some carriers. The Annex A specification is primarily a specification for outside North America.

Encapsulation and Fragmentation

RFC 1490 describes an encapsulation method for carrying packets across a Frame Relay network. All protocol packets are encapsulated within a Q.922 Annex A frame (a CCITT specification for data frames). The frames must also contain information necessary to identify the protocol being carried, allowing the receiver to properly process the incoming packets.

RFC 1490 also specifies a packet fragmentation and reassembly procedure for carrying frames over a Frame Relay network which are larger than the network's maximum frame size.

Note: RFC 1490 compliant devices from different vendors should interoperate with each other.

Network Protocol Addressing and Virtual Interfaces

Routing between LANs across a Frame Relay network is similar to routing across a point-to-point connection. A PVC on one router is directly connected to a PVC on another router. The difference with Frame Relay is that multiple PVCs can be supported on the same physical interface of a router.

Network protocol addresses are associated with each PVC using one of two methods: manual configuration or auto-discovery (Netopia's SmartMatch™).

Auto-discovery consists of two mechanisms: Inverse Address Resolution Protocol (InARP) and IP/IPX Routing Information Protocol (RIP) requests.

InARP, as outlined in RFC 1293, allows dynamic mapping of protocol addresses to a DLCI. It can be used for any network protocol, but is most commonly implemented for IP protocol.

When a router discovers a new, active PVC by communicating with the Frame Relay switch using the LMI protocol, it uses InARP to discover the IP address of the remote router on the other end of the PVC, when the PVC becomes active.

However, not all devices support InARP, so IP/IPX RIP is more common. The source address of the RIP response packet gives the Netopia R3100 the other router's address. In contrast, manual configuration involves manually configuring the association between the PVC DLCI and network protocol addresses. However, auto-discovery is the preferred configuration method because it is easier to set up than manual configuration.

Frame Relay partial mesh support

The following diagram depicts a partially meshed Frame Relay network:

2.0.0.1	router 1	1.0.0.1		1.0.0.2	router 2	3.0.0.1
4.0.0.1	router 3	1.0.0.3		1.0.0.4	router 4	5.0.0.1
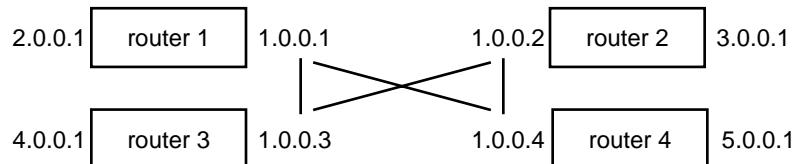
Note that the four routers above are connected in a partial mesh, all on the same IP network (1.0.0.0/24). Router 1 and router 2 cannot communicate directly, because there is no PVC between them. However, they can communicate via router 3 or router 4. The same is true for router 3 and router 4, which can communicate via router 1 or router 2.

Another common partial mesh topology is the following "star" or "hub and spoke" configuration:

2.0.0.1	router 2	1.0.0.2		1.0.0.3	router 3	3.0.0.1
9.0.0.1	router 1	1.0.0.1	— 1.0.0.4		router 4	4.0.0.1
6.0.0.1	router 6	1.0.0.6		1.0.0.5	router 5	5.0.0.1
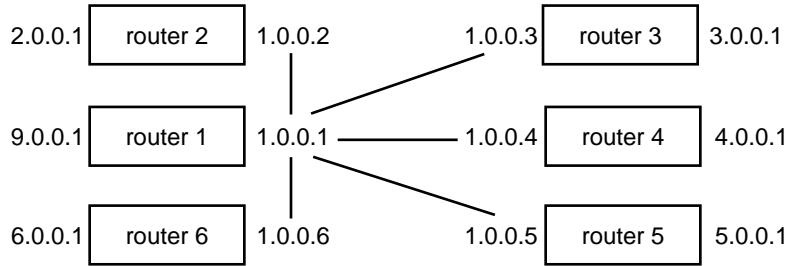
where there is connectivity among remote routers 2 through 6 and the networks behind them only via central site router 1.

Split horizon is a technique to reduce the possibility of routing loops that can occur due to network topology changes, such as when a router in the network fails.

Split-horizon means that the router does not propagate routes back to the subnet from which they were received. Poison-reverse means that it propagates routes back to the subnet from which they were received, but with a metric of 16 (unreachable).

Poison Reverse speeds convergence but adds to network overhead. When topology changes, mentioning routes that should not go through the router as well as those that should can speed up convergence.

If you select Split Horizon without Poison Reverse, the router omits routes learned from an interface from RIP updates sent on that interface. Split Horizon without Poison Reverse has the advantage of minimizing network overhead in large network configurations at the expense of slower convergence.

For example, consider a campus backbone connecting many buildings, each of which has a router. With Split Horizon without Poison Reverse, only the network that is connected to a router is included in the router's RIP updates. With Split Horizon with Poison Reverse, *all* networks will be included.

A partially meshed network is a WAN in which one or more nodes do not have logically direct connections to all other nodes. In a star or partially meshed Frame Relay topology, you may need to disable Split Horizon so the routers can learn about other networks.

Choose No Split Horizon for partial mesh frame relay networks where you have two or more PVCs that are connected to devices with IP addresses on the same subnet and are not directly connected by their own PVC. No Split Horizon is intended for use on any profile corresponding to a Frame Relay IP interface/subnet that has more than one DLCI that is not fully meshed. The effect is to suppress the normal Split Horizon behavior of RIP on that IP interface. This will ensure full connectivity on the partial mesh.

Appendix H

Event Histories

This appendix is a list of some of the events that can appear in the Netopia R3100's Event Histories. The text that appears in a history is shown in bold, followed by a brief explanation and the parameters associated with the event. The Event Histories display events for the Device and for the WAN under separate sections.

You can display more information about any event by selecting it in the Event History and pressing Return. See the example Device Event History shown below.

```
                      Device Event History

                                 Current Date --   6/4/97 09:23:53 AM
   -Date-----Time-----Event-------------------------------------------
   -------------------------------SCROLL UP----------------------------------
   06/04/97 08:56:13   AppleTalk initialization complete
   06/04/97 08:56:06   IPX initialization complete
   06/04/97 08:56:06   IP address server initialization complete
   06/04/97 08:56:06 --BOOT: Cold start-------------------------------------
   06/04/97 08:52:28   AURP initialization complete
   -------------------------------SCROLL DOWN--------------------------------

   Return/Enter on event item for details or 'SCROLL [UP/DOWN]' item for scrolling.
```

For example, if you select the BOOT event that occurred at 08:56:06 and press Return, the following popup screen appears:

```
        +----------------------EVENT DETAILS----------------------+
        +---------------------------------------------------------+
        |                                                         |
        | 08:56:06 on Wednesday, June 4, 1997                     |
        | --BOOT: Cold start------------------------------------- |
        |                 RETURN TO PREVIOUS MENU                 |
        |                                                         |
        +---------------------------------------------------------+
```
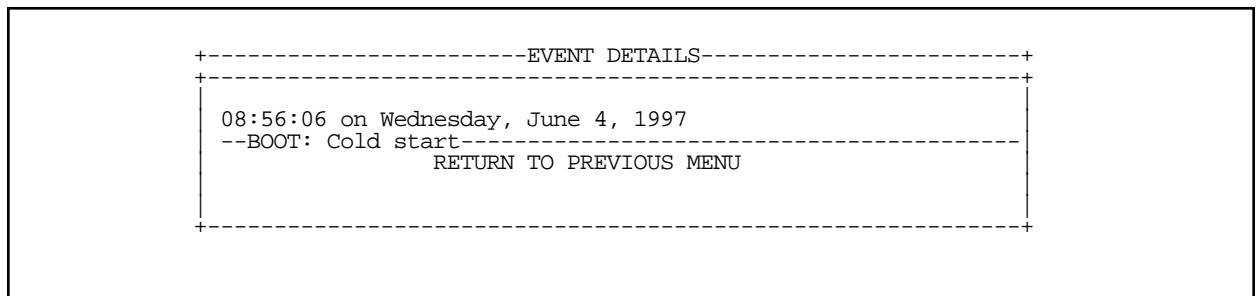
Leased line events

WAN data link activated at X Kbps: Indicates leased line is active at the specified speed (X).

WAN data link deactivated: Indicates leased line is not active.

ISDN events

ISDN Port Init: ISDN port has been initialized.

ISDN Line Active: ISDN L1 active - L1 not ready to carry L2 data. Associated parameter: switch type or protocol.

SPID Initialized: SPID accepted by switch. Associated parameter: directory number associated with SPID.

SPID Failed: SPID rejected/removed by switch. Associated parameter: directory number associated with SPID.

ISDN Line Deactivated: ISDN L1 not active - L1 not ready to carry L2 data. Associated parameter: switch type or protocol.

Received Clear Confirmation for our DN: Received clear confirmation from switch. Associated parameter: called directory number.

Received Clear Ind. from DN: Received clear indication from switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

Connection Confirmed to our DN: Received connect confirmation for Connect Request sent to the switch. Associated parameter: called directory number.

Received Connect Ind. for DN: Received connect indication for Call Request sent to the switch. Associated parameter: called directory number.

Received Disc. Ind. from DN: Received disconnect indication from switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

Received Setup Ind. from DN: Received call indication from switch. Associated parameter: called directory number.

Issued Setup Request from our DN: Call request was sent to switch. Associated parameter: called directory number.

Requested Connect to our DN: Connect request for the received call was sent to the switch. Associated parameter: called directory number.

Issued Clear Request for our DN: Clear request was sent to the switch. Associated parameter: called directory number.

Issued Clear Response to DN: Clear response was sent to the switch. Associated parameter: called directory number.

Disconnect Reqested: Disconnect request was sent to switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

ISDN event cause codes

These codes appear as associated (secondary) parameters in some of the ISDN events.

Cause No. 1: unallocated (unassigned number). This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned (allocated).

Cause No. 2: no route to specified transit network. This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular network, while it does exist, does not serve the equipment that is sending this cause.

This cause is supported on a network-dependent basis.

Cause No. 3: no route to destination. This cause indicates that the called user cannot be reached because the network through which the call has been routed does not serve the destination desired.

This cause is supported on a network-dependent basis.

Cause No. 6: channel unacceptable. This cause indicates that the channel used in this call is not acceptable to the sending entity.

Cause No.7: call awarded and being delivered in an established channel. This cause indicates that the user is receiving an incoming call, which is being connected to a channel already used by that user for similar calls (e.g., packet-mode X.25 virtual calls).

Cause No. 16: normal call clearing. This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.

Under normal situations, the source of this cause is not the network.

Cause No. 17: user busy. This cause is used when the called user has indicated the inability to accept another call.

It is noted that the user equipment is compatible with call.

Cause No. 18: no user responding. This cause is used when a user does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (defined in Recommendation Q.931 by the expiry of either timer T303 or T310).

Cause No. 19: no answer from user (user alerted). This cause is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time.

This cause is not necessarily generated by Q.931 procedures but may be generated by internal network timers.

Cause No. 21: call rejected. This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.

Cause No. 22: number changed. This cause is returned to a calling user when the called party number indicated by the calling user is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this capability, cause No. 1, unassigned (unallocated) number, shall be used.

Cause No. 26: non-selected user clearing. This cause indicates that the specified user has not been awarded the incoming call.

Cause No. 27: destination out of order. This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signaling message was unable to be delivered to the remote user: e.g., a physical layer or data link layer failure at the remote user, user equipment off-line, etc.

Cause No. 28: invalid number format (address incomplete). This cause indicates that the called user cannot be reached because the called party number is not a valid format or is not complete.

Cause No. 29: facility rejected. This cause is returned when a facility requested by the user cannot be provided by the network.

Cause No. 30: response to STATUS INQUIRY. This cause is included in the STATUS message when the reason for generated the STATUS message was the prior receive of a STATUS INQUIRY message.

Cause No. 31: normal, unspecified. This cause is used to report a normal even only when no other cause in the normal class applies.

Cause No. 34: no circuit/channel available. This cause indicates that there is no appropriate circuit/channel presently available to handle the call.

Cause No. 38: network out of order. This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time: e.g., immediately reattempting the call is not likely to be successful.

Cause No. 41: temporary failure. This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time: e.g., the user may wish to try another call attempt almost immediately.

Cause No. 42: switching equipment congestion. This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

Cause No. 43: access information discarded. This cause indicates that the network could not deliver access information to the remote user as requested: i.e., user-to-user information, low layer compatibility, high layer compatibility, or a sub-address as indicated in the diagnostic.

It is noted that the particular type of access information discarded is optionally included in the diagnostic.

Cause No. 44: requested circuit/channel not available. This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.

Cause No. 47: resource unavailable, unspecified. This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.

Cause No 49: Quality of Service not available. This cause is used to report that the requested Quality of Service, as defined in Recommendation X.213, cannot be provided (e.g., throughput or transit delay cannot be supported).

Cause No. 50: requested facility not subscribed. This cause indicates that the requested supplementary service could not be provided by the network because the user has not completed the necessary administrative arrangements with its supporting networks.

Cause No 57: bearer capability not authorized. This cause indicates that the user has requested a bearer capability implemented by the equipment that generated this cause that the user is not authorized to use.

Cause No. 58: bearer capability not presently available. This cause indicates that the user has requested a bearer capability implemented by the equipment that generated this cause which is not available at this time.

Cause No 63: service or option not available, unspecified. This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.

Cause No. 65: bearer capability not implemented. This cause indicates that the equipment sending this cause does not support the bearer capability requested.

Cause No. 66: channel type not implemented. This cause indicates that the equipment sending this cause does not support the channel type requested.

Cause No. 69: requested facility not implemented. This cause indicates that the equipment sending this cause does not support the requested supplementary service.

Cause No. 70: only restricted digital information bearer capability is available. This cause indicates that a device has requested an unrestricted bearer service but the equipment sending this cause only supports the restricted version of the requested bearer capability.

Cause No. 79: service or option not implemented, unspecified. This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.

Cause No. 81: invalid call reference value. This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.

Cause No. 82: identified channel does not exist. This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a primary rate interface numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.

Cause No. 83: a suspended call exists, but this call identify does not. This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).

Cause No. 84: call identity in use. This cause indicates that the network has received a call suspend request. The call suspend request contained a call identity (including the null call identity) which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.

Cause No. 85: no call suspended. This call indicates that the network has received a call resume request. The call resume request contained a call identity information element that presently does not indicate any suspended call within the domain interfaces over which calls may be resumed.

Cause No. 86: call having the requested call identity has been cleared. This cause indicates that the network has received a call resume request. The call resume request contained a call identity information element that once indicated a suspended call; however, that suspended call was cleared while suspended (either by network timeout or by remote user).

Cause No. 88: incompatible destination. This cause indicates that the equipment sending this cause has received a request to establish a call that has a low layer compatibility, high layer compatibility, or other compatibility attributes (e.g., data rate) that cannot be accommodated.

Cause No. 91: invalid transit network selection. This cause indicates that a transit network identification of an incorrect format as defined in Annex C/Q.931 was received.

Cause No. 95: invalid message, unspecified. This cause is used to report an invalid message event only when no other cause in the invalid message class applies.

Cause No. 96: mandatory information element is missing. This cause indicates that the equipment sending this cause has received a message that is missing an information element that must be present in the message before that message can be processed.

Cause No. 97: message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined but not implemented by the equipment sending this cause.

Cause No. 98: message not compatible with call state or message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.

Cause No. 99: information element non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message that includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

Cause No. 100: invalid information element contents. This cause indicates that the equipment sending this cause has received an information element which it has implemented; however, one or more of the fields in the information element are coded in a way that has not been implemented by the equipment sending this cause.

Cause No 101: message not compatible with call state. This cause indicates that a message has been received that is incompatible with the call state.

Cause No. 102: recovery on timer expiry. This cause indicates that a procedure has been initiated by the expiry of a timer in association with Q.931 error handling procedures.

Cause No. 111: protocol error, unspecified. This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

Cause No. 127: interworking, unspecified. This cause indicates there has been interworking with a network that does not provide causes for actions it takes; thus, the precise cause for a message being sent cannot be ascertained.

Appendix I

ISDN Configuration Guide

This appendix contains supplemental ISDN configuration information.

This section covers the following topics:

- ■ "Definitions" on page I-1
- ■ "About SPIDs" on page I-1
- ■ "Dynamic B-channel usage" on page I-2

Definitions

The following terms are used in this appendix:

Directory number: The actual phone number associated with the ISDN line you order. Depending on the type of switch protocol used on your line, there may be one directory number for both B-channels, or one for each B-channel.

SPID: The Service Profile ID generally looks like the directory number with some extra digits (the TID) appended to it. SPIDs are used only in North America. The number of SPIDs received from your ISDN service provider can vary from none to two.

TID (Terminal ID): This usually a four-digit number associated with the SPID. 0101 is the most popular, but it can vary in form. You may need to add a TID to each SPID you use when you configure the Netopia R3100.

If you encounter other unfamiliar terms, check the glossary.

About SPIDs

Depending on the type of ISDN switch protocol you use, you may be required to enter SPIDs in the ISDN Line Configuration screen. Generally, SPIDs are used with North American (United States and Canada) switch protocols.

The exact format of ISDN SPIDs is sometimes a point of confusion. This is because several formats exist, and some formats allow variations.

The table below displays the general SPID formats for the types of North American ISDN switch protocols supported by the Netopia R3100. The formats shown are a subset of possible SPID formats, but in most cases they should work.

In the following table, xxxxxxx represents the directory number assigned to your ISDN line, and yyy represents your area code.

Switch	SPID format
AT&T 5ESS custom (multipoint)	01xxxxxxx0

Switch	SPID format
Northern Telecom DMS-100 custom	yyyxxxxxxx1 and yyyxxxxxxx2 or yyyxxxxxxx01 and yyyxxxxxxx02
National ISDN-1 on AT&T 5ESS (multipoint)	01xxxxxxx000
National ISDN-1 on Northern Telecom DMS-100	yyyxxxxxxx0100 and yyyxxxxxxx0101

Note: AT&T 5ESS custom point-to-point switches have no SPIDs and are not represented in the table above. However, this type of switch configuration is supported by the Netopia R3100.

Example SPIDs

If your ISDN line is controlled by a DMS-100 switch using National ISDN-1, and your directory numbers are given as (415)234-5678 and (415)234-5679, your SPIDs are 41523456780101 and 41523456790201. Alternately, your SPIDs can be 41523456780100 and 41523456790200, but these are unusual, and rarely seen in new installations.

Dynamic B-channel usage

If the **B-Channel Usage** item in a connection profile's PPP/MP Options screen is set to **Dynamic** or **2 B, Pre-emptible**, one or both B channels may be in use at any time during a call made with that connection profile. Use of the second B-channel depends on traffic volume.

In addition, one of the B-channels may be relinquished if there is an incoming call, or if a second outgoing connection is made using another connection profile.

The ability to allow incoming calls when both B-channels are in use depends on the type of switch protocol on the local ISDN line, and how that line is provisioned (configured). Some types of switch protocols never allow incoming calls when both B-channels are in use. Switch protocols that do allow incoming calls must have the additional call offering (ACO) parameter turned on for data. ACO for data is off by default.

The table below shows which supported switch types can allow an incoming call when ACO for data is on.

Type of switch:	Incoming call allowed?
AT&T 5ESS custom	N/A
AT&T 5ESS National ISDN-1	Yes
DMS-100 custom	Yes*
DMS-100 National ISDN-1	Yes*

* Must have two directory numbers assigned.

This table may not be a complete list of switch protocols that support ACO. To find out if your switch protocol supports ACO, or to turn ACO on, contact your ISDN service provider.

Other incoming call restrictions

A B-channel will not be relinquished to admit an incoming call if a connection profile has **B-Channel Usage** set to **2 B-Channels**.

A B-channel will not be relinquished to admit an incoming call when there are two separate concurrent calls. Incoming calls are automatically allowed in when there is at least one B-channel free.

Appendix J

Binary Conversion Table

This table is provided to help you choose subnet numbers and host numbers for IP and MacIP networks that use subnetting for IP addresses.

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
0	0	32	100000	64	1000000	96	1100000
1	1	33	1000001	65	1000001	97	1100001
2	10	34	100010	66	1000010	98	1100010
3	11	35	100011	67	1000011	99	1100011
4	100	36	100100	68	1000100	100	1100100
5	101	37	100101	69	1000101	101	1100101
6	110	38	100110	70	1000110	102	1100110
7	111	39	100111	71	1000111	103	1100111
8	1000	40	101000	72	1001000	104	1101000
9	1001	41	101001	73	1001001	105	1101001
10	1010	42	101010	74	1001010	106	1101010
11	1011	43	101011	75	1001011	107	1101011
12	1100	44	101100	76	1001100	108	1101100
13	1101	45	101101	77	1001101	109	1101101
14	1110	46	101110	78	1001110	110	1101110
15	1111	47	101111	79	1001111	111	1101111
16	10000	48	110000	80	1010000	112	1110000
17	10001	49	110001	81	1010001	113	1110001
18	10010	50	110010	82	1010010	114	1110010
19	10011	51	110011	83	1010011	115	1110011
20	10100	52	110100	84	1010100	116	1110100
21	10101	53	110101	85	1010101	117	1110101
22	10110	54	110110	86	1010110	118	1110110
23	10111	55	110111	87	1010111	119	1110111
24	11000	56	111000	88	1011000	120	1111000
25	11001	57	111001	89	1011001	121	1111001
26	11010	58	111010	90	1011010	122	1111010
27	11011	59	111011	91	1011011	123	1111011
28	11100	60	111100	92	1011100	124	1111100
29	11101	61	111101	93	1011101	125	1111101
30	11110	62	111110	94	1011110	126	1111110
31	11111	63	111111	95	1011111	127	1111111

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

Appendix K

Further Reading

Angell, David. *ISDN for Dummies*, Foster City, CA: IDG Books Worldwide, 1995. Thorough introduction to ISDN for beginners.

Apple Computer, Inc. *AppleTalk Network System Overview*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1989.

Apple Computer, Inc. *Planning and Managing AppleTalk Networks*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1991.

Black, U. *Data Networks: Concepts, Theory and Practice*. Englewood Cliffs, New Jersey: Prentice Hall; 1989.

Black, U. *Physical Level Interfaces and Protocols*. Los Alamitos, California: IEEE Computer Society Press; 1988.

Black, Uyless. *Emerging Communications Technologies*, Englewood Cliffs, New Jersey: PTR Prentice Hall, 1994. Describes how emerging communications technologies, including ISDN and Frame Relay operate and where they fit in a computer/communications network.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Network Management and the Design of SNMP." ConneXions: The Interoperability Report, Vol. 3: March 1989.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Introduction to the Simple Gateway Monitoring Protocol." IEEE Network: March 1988."

Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*, Sebastopol, CA: O'Reilly & Associates, 1995. Dense and technical, but Chapter 6 provides a basic introduction to packet filtering.

Chapman, D. Brent. "Network (In)Security Through IP Packet Filtering," paper available from Great Circle Associates, 1057 West Dana Street, Mountain View, CA 94041

Chappell, L. *Novell's Guide to NetWare LAN Analysis*. San Jose, California: Novell Press; 1993.

Clark, W. "SNA Internetworking." ConneXions: The Interoperability Report, Vol. 6, No. 3: March 1992.

Coltun, R. "OSPF: An Internet Routing Protocol." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

Comer, D.E. *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, Vol. I, 2nd ed. Englewood Cliffs, New Jersey: Prentice Hall; 1991.

Davidson, J. *An Introduction to TCP/IP*. New York, New York: Springer-Verlag; 1992.

Ferrari, D. *Computer Systems Performance Evaluation*. Englewood Cliffs, New Jersey: Prentice Hall; 1978.

Garcia-Luna-Aceves, J.J. "Loop-Free Routing Using Diffusing Computations." Publication pending in IEEE/ACM Transactions on Networking, Vol. 1, No. 1, 1993.

Garfinkel, Simson. *PGP: Pretty Good Privacy*, Sebastopol, CA: O'Reilly & Associates, 1991. A guide to the free data encryption program PGP and the issues surrounding encryption.

Green, J.K. *Telecommunications*, 2nd ed. Homewood, Illinois: Business One Irwin; 1992.

Hagans, R. "Components of OSI: ES-IS Routing." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

Hares, S. "Components of OSI: Inter-Domain Routing Protocol (IDRP)." ConneXions: The Interoperability Report, Vol. 6, No. 5: May 1992.

Jones, N.E.H. and D. Kosiur. *Macworld Networking Handbook*. San Mateo, California: IDG Books Worldwide, Inc.; 1992.

Joyce, S.T. and J.Q. Walker II. "Advanced Peer-to-Peer Networking (APPN): An Overview." ConneXions: The Interoperability Report, Vol. 6, No. 10: October 1992.

Kousky, K. "Bridging the Network Gap." LAN Technology, Vol. 6, No. 1: January 1990.

LaQuey, Tracy. *The Internet Companion: A Beginner's Guide to Global Networking*, Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1994.

Leinwand, A. and K. Fang. *Network Management: A Practical Perspective*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1993.

Levine, John R. and Carol Baroudi. *The Internet for Dummies*, Foster City, CA: IDG Books Worldwide, 1993. Covers all of the most popular Internet services, including e-mail, newsgroups, and the World Wide Web. Also has information on setting up individual workstations with TCP/IP stacks.

Lippis, N. "The Internetwork Decade." Data Communications, Vol. 20, No. 14: October 1991.

McNamara, J.E. *Local Area Networks*. Digital Press, Educational Services, Digital Equipment Corporation, 12 Crosby Drive, Bedford, MA 01730.

Malamud, C. *Analyzing DECnet/OSI Phase V*. New York, New York: Van Nostrand Reinhold; 1991.

Malamud, C. *Analyzing Novell Networks*. New York, New York: Van Nostrand Reinhold; 1991.

Malamud, C. *Analyzing Sun Networks*. New York, New York: Van Nostrand Reinhold; 1991.

Martin, J. *SNA: IBM's Networking Solution*. Englewood Cliffs, New Jersey: Prentice Hall; 1987.

Martin, J., with K.K. Chapman and the ARBEN Group, Inc. *Local Area Networks. Architectures and Implementations*. Englewood Cliffs, New Jersey: Prentice Hall; 1989.

Medin, M. "The Great IGP Debate--Part Two: The Open Shortest Path First (OSPF) Routing Protocol." ConneXions: The Interoperability Report, Vol. 5, No. 10: October 1991.

Meijer, A. *Systems Network Architecture: A tutorial*. New York, New York: John Wiley & Sons, Inc.; 1987.

Miller, A. Mark. *Analyzing Broadband Networks (Frame Relay, SMDS, & ATM)*, M&T Books: A Division of MIS: Press, 1994. An intermediate/advanced reference on Frame Relay technologies.

Miller, M.A. *Internetworking: A Guide to Network Communications* LAN to LAN; LAN to WAN, 2nd. ed. San Mateo, California: M&T Books; 1992.

Miller, M.A. *LAN Protocol Handbook*. San Mateo, California: M&T Books; 1990.

Miller, M.A. *LAN Troubleshooting Handbook*. San Mateo, California: M&T Books; 1989.

O'Reilly, T. and G. Todino. *Managing UUCP and Usenet, 10th ed.* Sebastopol, California: O'Reilly & Associates, Inc.; 1992.

Perlman, R. *Interconnections: Bridges and Routers*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1992.

Perlman, R. and R. Callon. "The Great IGP Debate--Part One: IS-IS and Integrated Routing." ConneXions: The Interoperability Report, Vol. 5, No. 10: October 1991.

Rose, M.T. *The Open Book: A Practical Perspective on OSI*. Englewood Cliffs, New Jersey: Prentice Hall; 1990.

Rose, M.T. *The Simple Book: An Introduction to Management of TCP/IP-based Internets*. Englewood Cliffs, New Jersey: Prentice Hall; 1991.

Ross, F.E. "FDDI-A Tutorial." IEEE Communications Magazine, Vol. 24, No. 5: May 1986.

Schlar, S.K. *Inside X.25: A Manager's Guide*. New York, New York: McGraw-Hill, Inc.; 1990.

Schwartz, M. *Telecommunications Networks: Protocols, Modeling, and Analysis*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1987.

Sherman, K. *Data Communications: A User's Guide*. Englewood Cliffs, New Jersey: Prentice Hall; 1990.

Sidhu, G.S., R.F. Andrews, and A.B. Oppenheimer. *Inside AppleTalk, 2nd ed.* Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1990.

Siyan, Karanjit. *Internet Firewall and Network Security*, Indianapolis: New Riders Publishing, 1995. Similar to the Chapman and Zwicky book.

Smith, Philip. *Frame Relay Principles and Applications*, Addison-Wesley Publishing Company, 1996. Covers information on Frame Relay, including the pros and cons of the technology, description of the theory and application, and an explanation of the standardization process.

Spragins, J.D. et al. *Telecommunications Protocols and Design*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1991.

Stallings, W. *Data and Computer Communications*. New York, New York: Macmillan Publishing Company; 1991.

Stallings, W. *Handbook of Computer-Communications Standards,* Vols. 1-3. Carmel, Indiana: Howard W. Sams, Inc.; 1990.

Stallings, W. *Local Networks*, 3rd ed. New York, New York: Macmillan Publishing Company; 1990.

Stevens, W.R. *TCP/IP Illustrated*, Vol 1. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1994.

Sunshine, C.A. (ed.). *Computer Network Architectures and Protocols*, 2nd ed. New York, New York: Plenum Press; 1989.

Tannenbaum, A.S. *Computer Networks*, 2nd ed. Englewood Cliffs, New Jersey: Prentice Hall; 1988.

Terplan, K. *Communication Networks Management*. Englewood Cliffs, New Jersey: Prentice Hall; 1992.

Tsuchiya, P. "Components of OSI: IS-IS Intra-Domain Routing." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

Tsuchiya, P. "Components of OSI: Routing (An Overview)." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

Zimmerman, H. "OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection." IEEE Transactions on Communications COM-28, No. 4: April 1980.

Appendix L

Technical Specifications and Safety Information

Pinouts for Auxiliary Port Modem Cable
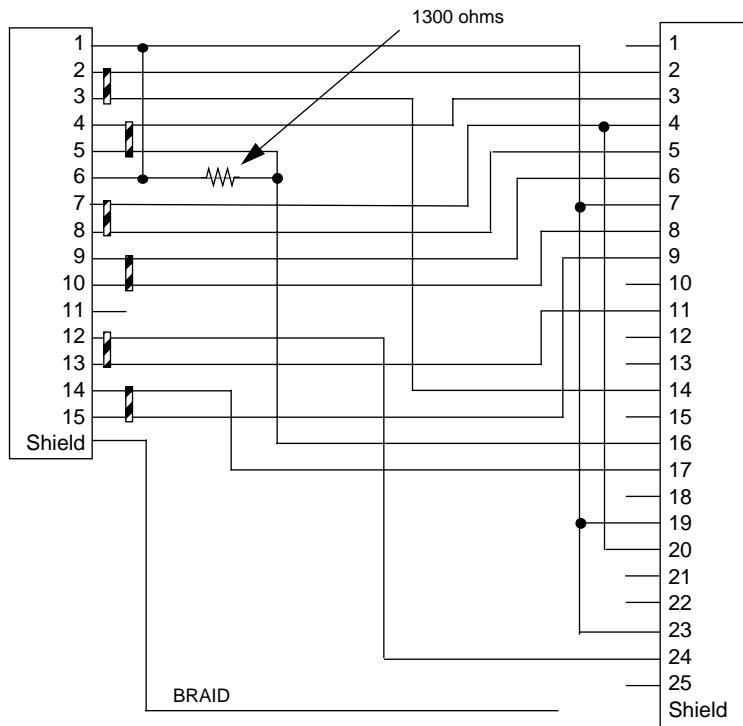
HD-15		DB-25	
Pin 1	Ground	Pin 1	(not used)
Pin 2	TDA	Pin 2	TD
Pin 3	TDB	Pin 3	RD
Pin 4	RDA	Pin 4	RTS
Pin 5	RDB	Pin 5	CTS
Pin 6	(not used)	Pin 6	DCE Ready
Pin 7	DTR	Pin 7	Ground
Pin 8	CTS	Pin 8	RLSD

HD-15		DB-25	
Pin 9	DSR	Pin 9	-RSET (EIA-530)
Pin 10	DCD	Pin 10	(not used)
Pin 11	(not used)	Pin 11	-TSET (EIA-530)
Pin 12	TCA	Pin 12	(not used)
Pin 13	TCB	Pin 13	(not used)
Pin 14	RCA	Pin 14	-TD (EIA-530) STD (EIA-232)
Pin 15	RCB	Pin 15	(not used)
		Pin 16	-RD (EIA-530) SRD (EIA-232)
		Pin 17	RSET
		Pin 18	(not used)
		Pin 19	-RTS (EIA-530) SRTS (EIA-232)
		Pin 20	DTE Ready
		Pin 21	(not used)
		Pin 22	(not used)
		Pin 23	Ground
		Pin 24	TSET
		Pin 25	(not used)
Note: Certain RS-232 modems do not properly accept signals on pins 12/24, 13/11, 14/17, and 15/9. For these applications, these pins may need to be cut.			

Description

Dimensions: 124.0 cm (w) x 20.0 cm (d) x 5.3 cm (h)
9.4″ (w) x 7.9″ (d) x 2.1″ (h)

Communications interfaces: The Netopia R3100 ISDN Router has an RJ-45 jack for ISDN connections; an 8 port 10Base-T Ethernet hub for your LAN connection; a DE-9 Console port; and an HD-15 Auxiliary port that can be used as either a serial or LocalTalk port.

Power requirements

- 12 VDC input
- 1.5 Amps

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% non-condensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via XMODEM or TFTP

Routing: TCP/IP Internet Protocol Suite, RIP, AppleTalk*, LocalTalk-to-Ethernet routing*, AURP tunneling*, MacIP*, IPX

* optional add-on feature

WAN support: PPP, MP, HDLC, Frame Relay

Security: PAP, CHAP, PAP-TOKEN, CACHE-TOKEN, callback, SecurID, IP/IPX firewalls, UI password security, and CallerID

SNMP network management: SNMPv1, MIB-II (RFC 1213), Interface MIB (RFC 1229), Ethernet MIB (RFC 1643), AppleTalk MIB-I (1243), Netopia R3100 MIB

Management/configuration methods: HTTP (web server), serial console, remote modem console, telnet, SNMP

Diagnostics: PING, event logging, routing table displays, traceroute, statistics counters, Call Accounting

Agency approvals

North America

Safety Approvals:

- United States – UL: 1950 Third Edition
- Canada – CSA: CAN/CSA-C22.2 No. 950-95

EMI:

- FCC Class A

International

Safety Approvals:

- Low Voltage (European directive) 72/23
- EN60950 (Europe)
- ETSI 300 047 (Europe)
- AS/NRZ 3260 (Australia)
- TS001(Australia)
- TS008 (Australia)

EMI Compatibility:

- 89/336/EEC (European directive)
- EN55022:1994   CISPR22 Class B
- EN550082-1:1992 (Immunity)

Network Homologation:

- Telecom Terminal Equipment, 91/263/EEC (European directive): CTR3
- TS031 (Australia)

Regulatory notices

Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

United States. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Requirements, Part 68. The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.

If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.

The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.

If the telephone company requests information on what equipment is connected to their lines, inform them of:

   a) The telephone number to which this unit is connected.

   b) The ringer equivalence number

   c) The USOC jack required. (RJ11C)

   d) The FCC Registration Number. (14 digits provided by FCC)

Items (b) and (d) are indicated on the label. The Ringer Equivalence Number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the REN's of all devices on any one line should not exceed five (5.0). If too many devices are attached, they many not ring properly.

Service Requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or our of warranty. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 2470 Mariner Square Loop, Alameda, California, 94501.

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Declaration for Canadian users

The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord.) The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100.

Important safety instructions

Australian Safety Information

The following safety information is provided in conformance with Australian safety requirements:

CAUTION: DO NOT USE BEFORE READING THE INSTRUCTIONS: Do not connect the Ethernet, Phone 1 and Phone 2 ports to a carrier or carriage service provider's telecommunications network or facility unless: a) you have the written consent of the network or facility manager, or b) the connection is in accordance with a connection permit or connection rules.

Connection of the Ethernet, Phone 1, and Phone 2 ports may cause a hazard or damage to the telecommunication network or facility, or persons, with consequential liability for substantial compensation.

Caution

■   The direct plug-in power supply serves as the main power disconnect; locate the direct plug-in power supply

near the product for easy access.

■ For use only with CSA Certified Class 2 power supply, rated 12VDC, 1.5A.

Telecommunication installation cautions

■ Never install telephone wiring during a lightning storm.

■ Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

■ Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

■ Use caution when installing or modifying telephone lines.

■ Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

■ Do not use the telephone to report a gas leak in the vicinity of the leak.

Battery

The Netopia R3100's lithium battery is designed to last for the life of the product. The battery is not user-serviceable.

Caution!

Danger of explosion if battery is incorrectly replaced.

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Glossary

Access Line: A telephone line reaching from the telephone company central office to a point usually on your premises. Beyond this point the wire is considered inside wiring. See also *Trunk Line.*

analog: In telecommunications, telephone transmission and/or switching that is not digital. An analog phone transmission is one that was originally intended to carry speech or voice, but may with appropriate modifications be used to carry data of other types.

ANSI (American National Standards Institute): Devises and proposes recommendations for international communications standards. See also *Comite Consultatif International Telegraphique et Telephonique (CCITT*).

AppleTalk: A comprehensive network system designed and developed by Apple Computer, Inc. AppleTalk allows many different types of computer systems, printers, and servers to communicate on a variety of cabling schemes, including LocalTalk and Ethernet cabling. In this manual, AppleTalk refers especially to the protocols or rule sets that govern this communication.

AppleTalk address: A unique identifier for each device using AppleTalk that allows information to be sent and received correctly. An AppleTalk address always includes a network number wherever two or more AppleTalk networks are connected together by routers.

AURP (Apple Update-based Router Protocol): An enhanced AppleTalk routing protocol. AURP provides improved support for AppleTalk over wide area networks (WANs) and tunneling through non-AppleTalk (IP) networks. AURP features include network number remapping, clustering of remote network numbers, and hop count reduction.

backbone: A network topology consisting of a single length of cable with multiple network connection points.

Bandwidth: The range of frequencies, expressed in Kilobits per second, that can pass over a given data transmission channel within a network. The bandwidth determines the rate at which information can be sent through a channel - the greater the bandwidth, the more information that can be sent in a given amount of time.

BAP: Bandwidth Allocation Protocol. Manages the dynamic bandwidth allocation of implementations supporting the PPP multilink protocol. This is done by defining the Bandwidth Allocation Protocol (BAP), as well as its associated control protocol, the Bandwidth Allocation Control Protocol (BACP). BAP can be used to manage the number of links in a multilink bundle.

baud rate: The rate of the signaling speed of a transmission medium.

bit: A binary digit; the smallest unit of data in the binary counting system. A bit has a value of either 0 or 1.

bits per second (bps): A measure of the actual data transmission rate. The bps rate may be equal to or greater than the baud rate depending on the modulation technique used to encode bits into each baud interval. The correct term to use when describing modem data transfer speeds.

bps: See *bits per second.*

branch: A length of cable in a star network that goes from the center of the star to a wall jack.

broadcast: A network transaction that sends data to all hosts connected to the network.

Burstiness: Data that uses bandwidth only sporadically; that is, information that does not use the total bandwidth of a circuit 100 percent of the time. During pauses, channels are idle; and no traffic flows across them in either direction. Interactive and LAN-to-LAN data is bursty in nature, because it is sent intermittently, and in between data transmission the channel experiences idle time waiting for the DTEs to respond to the transmitted data user's input of waiting for the user to send more data.

byte: A group of bits, normally eight, which represent one data character.

CallerID: See *CND.*

CCITT (Comite Consultatif International Telegraphique et Telephonique): International Consultative Committee for Telegraphy and Telephony, a standards organization that devises and proposes recommendations for international communications. See also *ANSI (American National Standards Institute).*

CHAP (challenge handshake protocol): A method for ensuring secure network access and communications.

Class A, B, and C networks: The values assigned to the first few bits in an IP network address determine which class designation the network has. In decimal notation, Class A network addresses range from 1.X.X.X to 126.X.X.X, Class B network addresses range from 128.1.X.X to 191.254.X.X, and Class C addresses range from 192.0.1.X to 223.255.254.X. For more information on IP network address classes, see Appendix E, "Understanding IP Addressing."

client: An intelligent workstation that makes requests to other computers known as servers. PC computers on a LAN can be clients.

clustering: A feature that clusters remapped network numbers into a range of sequential network numbers.

CNA (Calling Number Authentication): A security feature that will reject an incoming call if it does not match the Calling Number field in one of the Netopia ISDN Router's Connection Profiles.

CND (Calling Number Delivery):   Also known as caller ID, a feature that allows the Called Customer Premises Equipment (CPE) to receive a calling party's directory number during the call establishment phase.

community strings: Sequences of characters that serve much like passwords for devices using SNMP. Different community strings may be used to allow an SNMP user to gather device information or change device configurations.

CRC (Cyclic Redundancy Check): A computational means to ensure the integrity of a block of data. The mathematical function is computed, before the data is transmitted at the originating device. Its numerical value is computed based on the content of the data. This value is compared with a recomputed value of the function at the destination device.

DCE (Data Communications Equipment): Term defined by standards committees, that applies to communications equipment, typically modems or printers, as distinct from other devices that attach to the network, typically personal computers or data terminals (DTE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Also see *DTE.*

DDP (Datagram Delivery Protocol):   Defines socket-to-socket delivery of datagrams over an AppleTalk internet.

DTE (Data Terminal Equipment): Term defined by standards committees, that applies to communications equipment, typically personal computers or data terminals, as distinct from other devices that attach to the network, typically modems or printers (DCE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Pins 2 and 3 are reversed. Also see *DCE.*

default zone: When a Phase II EtherTalk network includes more than one zone, all routers on that network must be configured to assign one of these zones as a default zone. The default zone is temporarily assigned to any Phase II EtherTalk node that hasn't chosen a zone. The user may choose another zone by opening the Network Control Panel, selecting the correct physical connection, and then choosing a zone in the scrolling field displayed.

DHCP (Dynamic Host Configuration Protocol): A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DNS (Domain Name Service): A TCP/IP protocol for discovering and maintaining network resource information distributed among different servers.

download: The process of transferring a file from a server to a client.

EIA (Electronic Industry Association): A North American standards association.

Ethernet: A networking protocol that defines a type of LAN characterized by a 10 Mbps (megabits per second) data rate. Ethernet is used in many mainframe, PC, and UNIX networks, as well as for EtherTalk.

Ethernet address: Sometimes referred to as a hardware address. A 48-bits long number assigned to every Ethernet hardware device. Ethernet addresses are usually expressed as 12-character hexadecimal numbers, where each hexadecimal character (0 through F) represents four binary bits. Do not confuse the Ethernet address of a device with its network address.

EtherTalk: Apple's data-link software that allows an AppleTalk network to be connected by Ethernet cables. EtherTalk is a protocol within the AppleTalk protocol set. Two versions of EtherTalk are in common use, designated as Phase I and Phase II EtherTalk.

extended network: A network using AppleTalk Phase II protocols; EtherTalk 2.0 and TokenTalk are extended networks. LocalTalk networks are compatible with Phase II but are not extended because a single LocalTalk network cannot have multiple network numbers or multiple zone names.

firmware: System software stored in a device's memory that controls the device. The Netopia ISDN Router's firmware can be updated.

gateway: A device that connects two or more networks that use different protocols. Gateways provide address translation services, but do not translate data. Gateways must be used in conjunction with special software packages that allow computers to use networking protocols not originally designed for them.

hard seeding: A router setting. In hard seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information and the information provided by another router, it disables the router port for which there is a conflict. See also *non-seeding, seeding, seed router,* and *soft seeding.*

HDLC (High Level Data Link Control): A generic link-level communications protocol developed by the International Organization for Standardization (ISO). HDLC manages synchronous, code-transparent, serial information transfer over a link connection. See also *SDLC (Synchronous Data Link Control).*

header: In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

hop: A single traverse from one node to another on a LAN.

hop count: The number of nodes (routers or other devices) a packet has gone through. If there are six routers between source and destination nodes, the hop count for the packet will be six when it arrives at its destination node. The maximum allowable hop count is usually 15.

hop count reduction: A feature of AURP supported by the Netopia ISDN Router. Tunnels and point-to-point links over WANs can often exceed the maximum allowable hop count of 15 routers. Network administrators can use the hop count reduction feature to set up tunnels and point-to-point links that exceed the 15-router limit.

host: A single, addressable device on a network. Computers, networked printers, and routers are hosts.

Host Computer: A communications device that enables users to run applications programs to perform such functions as text editing, program execution, access to data bases, etc.

internet: A set of networks connected together by routers. This is a general term, not to be confused with the large, multi-organizational collection of IP networks known as the Internet. An internet is sometimes also known as an internetwork.

internet address, IP address: Any computing device that uses the Internet Protocol (IP) must be assigned an internet or IP address. This is a 32-bit number assigned by the system administrator, usually written in the form of 4 decimal fields separated by periods, e.g., 192.9.200.1. Part of the internet address is the IP network number (IP network address), and part is the host address (IP host address). All machines on a given IP network use the same IP network number, and each machine has a unique IP host address. The system administrator sets the subnet mask to specify how much of the address is network number and how much is host address. See also *Class A, B, and C networks*.

IP (Internet Protocol): A networking protocol developed for use on computer systems that use the UNIX operating system. Often used with Ethernet cabling systems. In this manual, IP is used as an umbrella term to cover all packets and networking operations that include the use of the Internet Protocol. See also *TCP/IP*.

IP address, IP host address, IP network address: See *internet address*.

IP broadcast: See *broadcast*.

IP tunneling: See *AURP*.

IPX (Internet Package Exchange): A protocol used by Novell Netware networks.

ISDN (Integrated Services Digital Network): A method of transmitting data digitally over telephone lines.

ISP (Internet service provider): A company that provides Internet-related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

ITU (International Telecommunication Union): United Nations specialized agency for telecommunications. Successor to CCITT.

K56flex: A modem data transmission technology standard created by Lucent Technologies and Rockwell International. Its purpose is to take advantage of the largely digital portions of the telephone system in order to exceed the theoretical speed limitations of data transmission over analog telephone lines. A competing technology called "x2," created by U.S. Robotics/3Com, performs a similar function. In February, 1998, the interested parties agreed on a unified standard called V.90, also known as V.PCM, which merges the K56flex standard with the competing x2 standard. In September, 1998, the International Telecommunications Union is expected to ratify the unified standard, thereby allowing interoperability of modems and ISPs' central site equipment, with appropriate firmware upgrades.

LAN (Local Area Network): A privately owned network that offers high-speed communications channels to connect information processing equipment in a limited geographic area.

LocalTalk: The cabling specification for AppleTalk running at a speed of 230.4 kbps (kilobits per second).

MacIP: A protocol in which IP packets are encapsulated within AppleTalk headers, for transmission over AppleTalk networks. MacIP requires the presence of at least one AppleTalk–IP gateway. MacIP is usually used to allow an AppleTalk computer to communicate with an IP computer.

MacIP client: A Macintosh computer that is using the MacIP protocol to communicate with an IP computer.

MIB (Management Information Base): A standardized structure for SNMP management information.

modem: A device used to convert digital signals from a computer into analog signals that can be transmitted across standard analog (not ISDN) telephone lines. Modem is a contraction of modulator-demodulator.

NAT (Network Address Translation): A feature that allows communication between the LAN connected to the Netopia ISDN Router and the Internet using a single IP address, instead of having a separate IP address for each computer on the network.

NetBIOS: A network communications protocol used on PC LANs.

network: A group of computer systems and other computer devices that communicate with one another.

network administrator: A person who coordinates the design, installation, and management of a network. A network administrator is also responsible for troubleshooting and for adding new users to the network.

network log: A record of the names of devices, location of wire pairs, wall-jack numbers, and other information about the network.

network number: A unique number for each network in an internet. AppleTalk network numbers are assigned by seed routers, to which the network is directly connected. An isolated AppleTalk network does not need a network number.

network number remapping: Resolves network number conflicts when two or more AppleTalk networks that may have duplicate network numbers are connected together. The Netopia ISDN Router lets you set up a range of network numbers into which remote AppleTalk network numbers are remapped.

network range: A unique set of contiguous numbers associated with an extended network; each number in a network range can be associated with up to 253 node addresses.

node: See *host*.

non-seeding: A router setting that causes it to request network number and zone information from any other routers on the network connected to the non-seeding port. If it receives this information, it begins to route packets through that port. See also *hard seeding, seeding, seed router,* and *soft seeding.*

packet: A group of fixed-length binary digits, including the data and call control signals, that are transmitted through an X.25 packet-switching network as a composite whole. The data, call control signals, and possible error control information are arranged in a predetermined format. Packets do not always travel the same pathway but are arranged in proper sequence at the destination side before forwarding the complete message to an addressee.

Packet-Switching Network: A telecommunications network based on packet-switching technology, wherein a transmission channel is occupied only for the duration of the transmission of the packet.

PAP (PPP authentication protocol): A method for ensuring secure network access.

Parameter: A numerical code that controls an aspect of terminal and/or network operation. Parameters control such aspects as page size, data transmission speed, and timing options.

port: A location for passing data in and out of a device, and, in some cases, for attaching other devices or cables.

port number: A number that identifies a TCP/IP-based service. Telnet, for example, is identified with TCP port 23.

POTS (Plain Old Telephone Service): Ordinary analog telephone service such as that used for voice transmission, as distinct from digital service.

PPP (Point to Point Protocol): A protocol for framing IP packets and transmitting them over a serial line.

protocol: A set of rules for communication, sometimes made up of several smaller sets of rules also called protocols. AppleTalk is a protocol that includes the LocalTalk, EtherTalk, and TokenTalk protocols.

remapping: See *network number remapping*.

RFC (Request for Comment): A series of documents used to exchange information and standards about the Internet.

RIP (Routing Information Protocol): A protocol used for the transmission of IP routing information.

RJ-11: A telephone-industry standard connector type, usually containing four pins.

RJ-45: A telephone-industry standard connector type usually containing eight pins.

router: A device that supports network communications. A router can connect identical network types, such as LocalTalk-to-LocalTalk, or dissimilar network types, such as LocalTalk-to-Ethernet. However—unless a gateway is available—a common protocol, such as TCP/IP, must be used over both networks. Routers may be equipped to provide WAN line support to the LAN devices they serve. They may also provide various management and monitoring functions as well as a variety of configuration capabilities.

router port: A physical or logical connection between a router and a network. Where a network only allows the use of one protocol, each physical connection corresponds to one logical router port. An example is the Netopia ISDN Router's LocalTalk port. Where a network allows the use of several protocols, each physical connection may correspond to several logical router ports—one for each protocol used. Each router port has its own network address.

routing table: A list of networks maintained by each router on an internet. Information in the routing table helps the router determine the next router to forward packets to.

seeding: A method for ensuring that two or more routers agree about which physical networks correspond to which network numbers and zone names. There are three options: non-seeding, soft seeding, and hard seeding. Seeding can often be set separately for each router port. See also *hard seeding*, *non-seeding, seed router,* and *soft seeding.*

seed router: A router that provides network number and zone information to any router that starts up on the same network. See also *hard seeding*, *non-seeding, seeding,* and *soft seeding.*

serial port: A connector on the back of the workstation through which data flows to and from a serial device.

server: A device or system that has been specifically configured to provide a service, usually to a group of clients.

SNMP (Simple Network Management Protocol): A protocol used for communication between management consoles and network devices. The Netopia ISDN Router can be managed through SNMP.

soft seeding: A router setting. In soft seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information for a particular port and the information provided by another router connected to that port, it updates its configuration using the information provided by the other router. See also *hard seeding*, *non-seeding, seeding,* and *seed router.*

subnet: A network address created by using a subnet mask to specify that a number of bits in an internet address will be used as a subnet number rather than a host address.

subnet mask: A 32-bit number to specify which part of an internet address is the network number, and which part is the host address. When written in binary notation, each bit written as 1 corresponds to 1 bit of network address information. One subnet mask applies to all IP devices on an individual IP network.

SDLC (Synchronous Data Link Control): A link-level communications protocol used in an International Business Machines (IBM) Systems Network Architecture (SNA) network that manages synchronous, code-transparent, serial information transfer over a link connection. SDLC is a subset of the more generic HDLC (High-Level Data Link Control) protocol developed by the International Organization for Standardization (ISO).

TCP/IP (Transmission Control Protocol/Internet Protocol): An open network standard that defines how devices from different manufacturers communicate with each other over one or more interconnected networks. TCP/IP protocols are the foundation of the Internet, a worldwide network of networks connecting businesses, governments, researchers, and educators.

telephone wall cable: 2-pair, 4-pair, or 8-pair, 22- or 24-gauge solid copper wire cable. Telephone wall cable is sometimes called telephone station cable or twisted-pair cable.

TFTP (Trivial File Transfer Protocol/Internet Protocol): A protocol used to transfer files between IP nodes. TFTP is often used to transfer firmware and configuration information from a UNIX computer acting as a TFTP server to an IP networking device, such as the Netopia ISDN Router.

thicknet: Industry jargon for 10Base-5 coaxial cable, the original Ethernet cabling.

thinnet: Industry jargon for 10Base-2 coaxial cable, which is thinner (smaller in diameter) than the original Ethernet cabling.

UDP (User Datagram Protocol): A TCP/IP protocol describing how packets reach applications in destination nodes.

V.90: A modem data transmission standard, also known as V.PCM, which merges the K56flex standard with the competing x2 standard. In September, 1998, the International Telecommunications Union is expected to ratify the unified standard, thereby allowing interoperability of modems and ISPs' central site equipment, with appropriate firmware upgrades.

wall jack: A small hardware component used to tap into telephone wall cable. An RJ-11 wall jack usually has four pins; an RJ-45 wall jack usually has eight pins.

WAN (wide area network): A network that consists of nodes connected by long-distance transmission media, such as telephone lines. WANs can span a state, a country, or even the world.

WAN IP: In addition to being a router, the Netopia ISDN Router is also an IP address server. There are four protocols it can use to distribute IP addresses over the WAN which include: DHCP, BOOTP, IPCP and MacIP. WAN IP is a feature for both the Small Office and Corporate Netopia ISDN Router models.

wiring closet: A central location where a building's telephone and network wiring is connected. Multi-story buildings often have a main wiring closet in the basement and satellite wiring closets on each floor.

zone: An arbitrary subset of nodes within an AppleTalk internet. Creating multiple zones makes it easier for users to locate network services. The network administrator defines zones when he or she configures routers. Isolated networks have no zones. LocalTalk and EtherTalk Phase I networks may have no more than one zone each. EtherTalk Phase II and TokenTalk networks may have more than one zone each. Several networks of any AppleTalk type may share a zone name.

Index

Limited Warranty and Limitation of Remedies

Netopia warrants to you, the end user, that the Netopia R3100™ ISDN Router (the "Product") will be free from defects in materials and workmanship under normal use for a period of one (1) year from date of purchase. Netopia's entire liability and your sole remedy under this warranty during the warranty period is that Netopia shall, at its sole option, either repair or replace the Product.

In order to make a claim under this warranty you must comply with the following procedure:

1. Contact Netopia Customer Service within the warranty period to obtain a Return Materials Authorization ("RMA") number.

2. Return the defective Product and proof of purchase, shipping prepaid, to Netopia with the RMA number prominently displayed on the outside of the package.

If you are located outside of the United States or Canada, please contact your dealer in order to arrange for warranty service.

THE ABOVE WARRANTIES ARE MADE BY NETOPIA ALONE, AND THEY ARE THE ONLY WARRANTIES MADE BY ANYONE REGARDING THE ENCLOSED PRODUCT. NETOPIA AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MER-CHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED PRODUCT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED ABOVE, NETOPIA AND ITS LICENSOR(S) DO NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE PRODUCT IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES OR JURISDICTIONS, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT CASE, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE PRODUCT. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM JURISDICTION TO JURISDICTION.

REGARDLESS OF WHETHER OR NOT ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL NETOPIA, ITS LICENSOR(S) AND THE DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS OF ANY OF THEM BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT THE USE OR INABILITY TO USE THE PRODUCT EVEN IF NETOPIA OR ITS LICENSOR(S) HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. NETOPIA AND ITS LICENSOR(S) LIABILITY TO YOU FOR ACTUAL DAMAGES FROM ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION (WHETHER IN CONTRACT, TORT [INCLUDING NEGLIGENCE], PRODUCT LIABILITY OR OTHERWISE), WILL BE LIMITED TO $50. v.0300